

AdvanIDe - Newsletter Issue No. 2 – October 2009

Introduction – by Holger Roessner, Managing Director

Dear reader,

Since our recent newsletter, our industry has gone through tremendous changes. What started with a breakdown of the real estate markets has finally reached the high tech sector with full brunt. Price erosions, inventory clearances and investment holds have affected our industry and hit especially hard those ones who are in the semiconductor supply chain. During those times, it is important to count on partners, who have creative ideas on how to solve problems and how to optimize the value chain.



We at AdvanIDe have taken great efforts during the last couple of months to work closely with our partners and customers to assist them during the downturn. We have experienced a great deal of understanding and were able to maneuver steadily and carefully. Currently, we do see some increase in lead times and factory loading factors, partially due to increased demand, but also due to a reduction of manufacturing capacities and the limitation of work in progress, which leads ultimately to longer manufacturing times. In the semiconductor industry, oversupply paired with a downturn of business and a sharp increase of demand coming along with shortages of supply or even an allocation situation both happen within a short time frame of only two months or so. In either way, it is important to be prepared and to have a specialized supply chain partner to assist during all cycles of the economy.

AdvanIDe is readily geared up to aid its partners and at this time, we would like to highlight again our excess management services for those partners who want to offload unused inventories.

Pls. also do feel free to forward this newsletter to colleagues and friends. We do look forward to an ever growing circle of [subscribers](#) to our newsletter.

Sincerely,



Contents:

- **News:** Partnership with ARE-CON
 - **AdvanIDe behind the scenes:** Walluf Office
 - **AdvanIDe in the media:** Cover Story at PassAgeNow & Executive Interview at CTnS Cards Leadership Forum
 - **Product Updates:** New products, useful links and documents
 - **Excess Stocks:** Special Offers for obsolete and excess parts from our customers – stock of SLE44 series ICs
 - **Article:** Migration path from Mifare Classic to Mifare PLUS – Upgrading the system
 - **From the desk of Line Management:** Current Trends in RFID Industry
 - **Partner Profile:** KSW
 - **Future Trends in Smart Card Industry:** from the Supplier's desk
 - **New Employees:** Frank Tekampe, Brian Niu, Oliver Stiegler and Carlo Ng
 - **Lucky Draw Result:** Winners of Nokia NFC Phones
-

News:

AdvanIDe appoints ARE-CON Value Added Reseller/VAR

The world's leading independent provider of silicon for RFID and chip card applications – AdvanIDe and Hatten/Germany based ARE-CON GmbH & Co. KG teamed up early this year to offer enhanced product and market coverage for customers of both companies.



ARE-CON's vast know how in the identification business segment and their added value products and services have played a major role in AdvanIDe selecting ARE-CON as a VAR. ARE-CON works with manufacturers of RFID inlays and laminates to serve card manufacturers and AdvanIDe provides components to the same customer group. More information about ARE-CON can be found here: www.aren-con.de and the team of ARE-CON is contactable under this link: www.aren-con.com/en/contact/

AdvanIDe behind the scenes:

Walluf – Regional Office for Europe and Africa Region and Base of Line Management Team

Located in Walluf, close to Frankfurt, our regional office for Europe and Africa serves its dedicated regions from the heart of Germany.

AdvanIDe GmbH as a successor of ACG Distribution is serving its markets for more than 10 years now. What started as ACG, a success story around smartcard identification systems for the electronic health card in Germany, soon developed into a dedicated distribution organization to serve card- and reader-manufacturers.



The office complex in Walluf serves as a regional headquarter for many other Assa Abloy companies as well. Being a shared location there are some shared functions as well. Most notably AdvanIDe is using the existing warehouse facilities to serve its customers throughout the region, which is well over 300 sq. mtr., in a high security environment and its close proximity to the airport in Frankfurt and its surrounding logistics industries makes it AdvanIDe's European hub.

Frank Tekampe is our Regional Sales Director. Frank has nine years of smartcard and identification industry experience, working formerly with ACG AG and ACG Distribution in various positions in sales and product management and was recently based in Sydney as Managing Director of BCDS. Frank holds a Master's Degree in Management (MSc) from the Macquarie Graduate School of Management, Sydney, Australia.

Johannes Borsch is our Sales Manager for France, Spain, Portugal, Italy, Benelux, Eastern Europe and Germany. Johannes is with our Distribution department since 2004. While dealing with customers directly Johannes is also taking care of our Value Added Reseller Advintec. Johannes is a proud father of two and likes to enjoy his weekends tending his house and backyard.

Volker Jansen is our Sales Manager for UK, Scandinavia, Germany, Greece, Turkey and Africa. Volker is with our Distribution team since 2004 as well. While dealing with customers directly Volker is also taking care of our

Value Added Reseller ARE CON. Volker was working as a purchase manager before joining and is also firm in Import and Export customs and declaration.

Jessica Stumm, our Customer Service Officer, is assisting our customers in those regions. Jessica has joined AdvanIDe in 2008. Jessica has just completed her bachelor professional after three years of part time studies at Schultze-Delitzsch-Schule in Wiesbaden.

Marcus Bug, our Purchasing and Customer Service Officer, is assisting our customers in those regions. Marcus has joint AdvanIDe end of 2007 and has been with Assa Abloy ITG before. Marcus started as an apprentice with ACG in 2004.

Holger Winterhalter, Head of Line Management, he is looking after all supplier related issues and acts as an interface between suppliers and sales. He is also leading the international team of field application engineers. Holger joined the group in 2004. He holds an Electrical Engineering degree.

Gaby Mönig, Line Manager for RFID, she is looking after the contactless business within AdvanIDe and also acts as a global interface between suppliers and sales. Gaby joined ACG in 2002 as Assistant Product Manager and has become Line Manager in 2005.

AdvanIDe in the media:

AdvanIDe was featured in the May/June Issue - Vol 3 No. 3 of PassAGENow.

For every end-product that ends up in the consumer's hands, the whole cycle of how the product was manufactured – from beginning till end – it is rarely of any real interest to the end user. To a vendor in the production chain however, it could be a critical point. Having a reliable and readily available source of materials is essential to ensure that production is unaffected, should any unforeseen incidents occur. The silicon industry is no different. The supply & demand for silicon fluctuates according to the market forces, thus vendors are sometimes caught in a difficult spot when demand outweighs supply. It is, in such situations, that a company has found its niche spot and excelled at it. Resourceful, independent and with a global reach, AdvanIDe has build up a solid reputation for being dependable and trustworthy. As the industry needs are constantly evolving, so has the company – expanding its repertoire to best support its customers in every way possible. Find out how this silicon broker is carving its mark in the contactless and RFID industry through the eyes of Holger Roessner, MD of AdvanIDe.



Pls. click [here](#) to read the full story.

AdvanIDe was featured in the September 09 Issue of CTnS Card Leadership Forum.

Smart cards and RFID tags are unique products in very special applications. The requirement for certified security like in the application of banking cards and credentials in electronic governance applications as well as the fact, that there is usually only one piece of silicon used in every piece of product makes the Smart Card and RFID segment a very special market place. Special enough for AdvanIDe which stands for Advanced ID Electronics to focus on this segment and acting as the first and only truly global distributor for silicon in ID and chip card applications.



Mr. Holger Roessner, worldwide Managing Director of AdvanIDe, is going to give our readers insights in AdvanIDe's business, its plans going forward and its relationships within the Chinese market place.

Pls. click [here](#) to read the full story.

Products:

New products, useful links and documents

MIFARE UltraLight C

MIFARE UltraLight C is the first smart card IC for limited-use applications that offers solution developers and providers the benefits of an open cryptography. With 3DES, MIFARE UltraLight C uses a widely adopted standard, enabling easy integration in existing infrastructures. The integrated authentication command set provides an effective cloning protection that helps to prevent counterfeit of tickets.

NXP MIFARE UltraLight C represents a new security concept to the contactless limited-use market. With its 3DES authentication, MIFARE UltraLight C reflects the trend for enhanced security in contactless applications. Nowadays many solution providers eliminate double infrastructure where MIFARE UltraLight C provides the perfect solution for a complete contactless system. It can easily be integrated in existing MIFARE DESFire installations, re-using similar authentication commands.



Key features:

- Fully ISO / IEC 14443 A 1-3 compliant
- 106 kbit/s communication speed
- Anti-collision support
- 1536 bits (192 bytes) EEPROM memory
- Protected data access via 3DES authentication
- Cloning protection
- Command set compatible to MIFARE UltraLight
- Memory structure as in MIFARE UltraLight (pages)
- 16 bit counter
- Unique 7 bytes serial number
- Number of single write operations: 10.000

Key Benefits:

- Ability to detect cloned tickets
- Availability of statistical data to optimize the system
- Efficient fleet management
- Higher customer throughput
- Reduction of maintenance costs
- Reduction of cash handling
- Fraud prevention
- Easy system enhancement in limited-use applications
- Compliance to ISO / IEC 14443 A 1-3
- Limited integration effort in MIFARE DESFire based solutions
- Enhanced security for limited-use applications
- Ease of use and proven toolkits
- Fast time-to-market

ICODE SLI-SY

National archives, university libraries and museums need an identification solution that will last for decades. Offering a guaranteed 40 years data retention, NXPs' ICODE SLI-SY answers this need. Building on the proven and reliable ICODE product family, this solution offers many additional benefits including benchmark read range and optional password security. ICODE SLI-SY features a range of security options which you can tailor to meet your application's requirements. You can use the IC without any password protection for example or you can leverage password protection to enable enhanced memory administration rights to prevent unauthorized writing and reading of classified data on the IC. It also features password-protected EAS functionality up to 32-bit passwords – letting you address the need for advanced theft protection. With 40 years guaranteed data retention, ICODE SLI-SY is the ideal choice for libraries, archives, long term asset management and other item-level tagging applications where items need to be stored for long periods of time. The long data retention brings significant added value for customers as label costs can be depreciated over a much longer time, giving a much better return on investment.

Building on the proven and reliable performance of our ICODE family, ICODE SLI-SY supports ISO 15693 as well as ISO 18000-3. It operates up to a distance of 2 meters, making it well suited for long-range applications, delivering a robust solution and quality of service.

Key features

- 40 years data retention
- Interface according to ISO 15693 / ISO 18000-3
- EAS functionality with optional password protection
- Optional and flexible password security concept for managing user memory access
- Password protected destroy and privacy functions
- 100% compatible with ICODE SLI-S

Key benefits

- 40 years data integrity guarantee
- Fully compliant with global standards and harmonized regulations
- Benchmark RF performance and reliability
- Addresses demands for customer privacy

PN533: NFC controller

NXP Semiconductors' PN533 is a highly integrated transmission module for contactless communication at 13.56 MHz based on 80C51 microcontroller core. It is specially designed to provide USB-enabled devices with the most widely deployed contactless communication protocols. PN533 supports following four operating modes:

- ISO/IEC 14443A Reader/Writer (Including MIFARE product family)
- ISO/IEC 14443B Reader/Writer
- FeliCa Reader/Writer
- ISO/IEC 18092, ECMA 340 Peer-to-Peer

Key features of PN533 are as below:

- Full peer-to-peer functionality
- Reader/ writer functionality compatible to ISO/IEC 14443 A&B, MIFARE, FeliCa and NFC Forum tag types (MIFARE UltraLight, Topaz, FeliCa, MIFARE DESFire)
- Card emulation functionality when connected to secure controller (P5CN072)
- Up to 10cm operating distance
- 80C51 core processor with embedded firmware
- USB host interface
- PN533 software is certified by Cetecom for eGovernment and by FIME for banking application
- NFC Sec for USB wireless and BT enabler support
- PC/SC driver WHQL pre-certified

PN544: NFC Controller

NXP has unveiled PN544; a new generation of Near Field Communication (NFC) controller chips which compliant with latest ETSI NFC specifications. NXP PN544 is primarily targeted to mobile phone manufacturers and operators to introduce next gen NFC devices and services. PN544 NFC controller enable cell phone users to access a new range of contactless applications such as mobile payments and paperless ticketing. PN544 also enable data sharing directly from the cell phone SIM (Subscriber Identity Module). PN544 NFC controller supports the three main architectures which are used to secure NFC transactions, including the Secure Element within the Universal Integrated Circuit Card (UICC), within the SD card and within the mobile handset.

Other key benefits of the PN544 NFC controller include:

- Shorter integration time due to qualified design-in support from NXP
- MIFARE 1K/4K Reader/writer functionality enabled in host baseband
- Optionally available with an modular, generic and platform independent software stack
- Optimized antenna designs for best-in-class RF performance

- Low power consumption
 - Working in Battery off and Battery Low modes
 - Small footprint
-

MF RX852: A secure Reader IC solution from NXP

MIFARE RX852 from NXP Semiconductors is the first low cost, secure reader IC solution of its kind. It is available for a wide range of contactless reader applications that will offer solution developers and providers the benefits of a system in package (SIP), multi-chip, secured contactless reader IC. With AES and 3DES support, MIFARE RX852 uses widely adopted and open standards, enabling easy and fast solution development of infrastructures.

The use of secure elements such as a secure application module (SAM) in a contactless reader enables the handling of different interfaces and security. Customers that target higher security requirements are now able to significantly reduce their implementation time with the new MIFARE RX852. Typically, the secure element is directly connected to a microcontroller, which handles the secured communication within a contactless reader. This additional interface causes a latency which negatively impacts the overall performance of the total system. With the MIFARE RX852, customers benefit from having a direct connection between the secure element and the contactless reader IC, which removes the latency effect and, therefore, improves the overall speed of a reader system. In general, it leads to reduced complexity, effort and cost of implementation and it allows customers to considerably cut time-to-market.

MF RX852 can be used in below Key application areas:

- Public transportation
- E-government
- Access management
- Point of Sales (POS)

Key features of MF RX852 are as below:

- ISO/ IEC 14443 A/B compliant
 - AES, 3DES, CRYPTO1 compatible
 - Multi-chip secured contactless reader IC
 - Secure key storage and key diversification
 - Contactless T=CL Protocol for MIFARE DESFire communication
-

Nokia 6216 Classic: SIM-based NFC phone

Nokia recently introduced the Nokia 6216 classic, a fully integrated, SIM-based Near Field Communication (NFC) device that lets operators build NFC services on the subscriber identity module (SIM) card. With one tap of the device, consumers can share mobile content with other Nokia 6216 classic phones and compatible NFC devices. For example, a consumer could store credit-card information on a device's SIM card and then make a quick payment by waving the device in front of a compatible contact-free terminal. The Nokia 6216 classic is based on Series 40 5th Edition, Feature Pack 1, and it implements the Contactless Communication API (JSR-257). Additional features include support for 8 GB micro SD cards, USB 2.0, Bluetooth 2.0 +EDR, Bluetooth stereo, Flash Lite 2.1, and MIDP Java 2.1 with additional Java APIs.



HITAG μ

NXP announced its latest low frequency RFID IC aimed at livestock identification and industrial logistics, the HITAG μ . The new IC offers the highest RF performance for effective tracking of livestock with industry benchmark read distances. Due to a fast write command feature the product has been optimized for initial set-up, reducing the programming time by half compared to other solutions on the market. The HITAG μ builds on

the concept and success of NXP's HITAG S IC, which has been leading in the market for low frequency RFID applications in the recent years. It is the first RFID chip for passive low frequency tags on the animal identification market to feature anti-collision technology. The algorithm ensures that multiple tags can be read at any given time allowing for individual animals in a herd to be identified. In other multiple tag applications, such as production control or asset management, the increased read distance, optimised anti-collision algorithm and reduced write times allow for a best in class identification solution, provided at competitive cost levels. The HITAG μ supports the existing ISO11784/85 and is fully compliant with the existing low frequency infrastructure in the market.

Key benefits for the HITAG μ include:

- Available in a new robust, affordable SOT (Small Outline Transistor) package, enabling all different assembly methods
- Optional security with 32-bit read and/or write password
- Enables global use through worldwide harmonized RF regulations – ISM band
- Unique NXP programmed 48 bit identifier
- Multiple User memory types
- 3% tolerance of resonance capacitance allowing mass production without tuning of antennas
- Multiple delivery forms including mega-bumped ICs and metal-straps

CardOS v4.4 on SLE66CX680PE

Siemens announced the discontinuation of the CardOS versions M4.01A, V4.2, V4.2B and V4.3B, due to the discontinuation of the P-platform by Infineon. The latest possible order date of CardOS M4.01A, V4.2, V4.2B and V4.3B, including the customer documentation and CardOS-ADK for these versions will be November 15th 2009. The latest possible delivery date would be February 28th, 2010. CardOS V4.2C is already being offered as a successor on Infineon's SLE66CX360PE for usage in projects without any certification requirements and CardOS V4.4 on the Infineon SLE66CX680PE is going to be available as certified version according to CC EAL4+, SSCD PP and German signature law in Fall 2009.

Features of CardOS V4.4

- Compatibility with international standards (ISO 7816)
- Specific versions are certified according to Common Criteria EAL4+ and German Signature Act (SigG) or CWA-14169
- Fast crypto operations and key generation on-card (true random number generator)
- Separate management of applications due to hierarchically structured file system
- Additional functions and algorithms can be simply added to the operating system due to the clearly structured, modular system architecture SLE66CX680PE hardware platform
- Crypto algorithms viz., RSA (2048 Bit key size), Triple-DES, SHA-1, AES (128, 192, 256 Bit key size), SHA 2 (incl. SHA 224, SHA 256) & Elliptic curves
- Fast on-card key generation modes
- Certification according to worldwide applicable Common Criteria security standard CC EAL4+ and Security Confirmation according to German Law (SigG) and CWA 14169 Type 3

Documents pertaining to the support information of migration to CardOS M4.01A, V4.2, V4.2B and V4.3B are available; please write to us at support@advanide.com.

Important Links:

- Tools and SDKs for Mobile Software Development
http://www.forum.nokia.com/Tools_Docs_and_Code/Tools/
- Online NFC training
http://www.nxp.com/technical_support/NFC/index.htm /

- RD701 Pegoda Reader Evaluation Software
[http://www.nxp.com/#/pip/pip=\[pip=HTRC11001T_2,pfp=41960\]|pp=\[t=pfp,i=41960\]](http://www.nxp.com/#/pip/pip=[pip=HTRC11001T_2,pfp=41960]|pp=[t=pfp,i=41960])
 - NFC Forum Technical Specifications
http://www.nfc-forum.org/specs/spec_list/
 - GlobalPlatform specifications
<http://www.globalplatform.org/specificationscard.asp>
-

Excess Stocks:

Special Offers for obsolete and excess parts

Dear readers,

We are now offering you an exclusive medium wherein any of your excess or odd lot stock will be put up for selling on our site for our viewers to view and request us for your lot. We request you to please submit your request for selling of the excess / odd lot stock at <http://www.advanide.com/excessstock/submitrequest.html>. The form looks like this and we request you to please provide detailed information as requested for a quick review. We expect about 24 hrs to have your request reviewed and put up on our site at <http://www.advanide.com/excessstock/stocklist.html>. Any request received by us from any of our customers, for your submitted lot, will be forwarded to you.

Also, we do have some excess stock, which we would like to have it sold as soon as possible. If you are interested, please write to us at info@advanide.com know for more information on the products.

Article:**Migration path from MIFARE Classic to MIFARE PLUS – Upgrading the system**

MIFARE, a trusted brand name in identification industry for ticketing applications, was launched in 1994. As of March 2009, more than 650 cities in more than 50 countries have adopted to MIFARE solutions. More than one billion cards have been issued, of which more than 800 million cards have been used as tickets. More than 10 million readers have been deployed in the field. This segment has been supported by more than 800 MIFARE solution providers consisting of card / reader makers, solution developers and system integrators. Apart from ticketing application, there are more than 40 application types have been developed and deployed across industry categories.

One must be wondering, why is all this being mentioned now in this article? Well, in the 24th Chaos Communication Congress, two Virginia University students showed how weak this Crypto1 algorithm is and how easily it could be broken. The goal of these presentations was to

prove that the Crypto1 algorithm, which was introduced in 1994, is now weak enough to be broken into using normal computers. It was a pointer to the industry to open their eyes and ask them to shift to some cryptography which is more complex and difficult to break.

After about thirteen years i.e., in 2007 someone was able to reverse the Crypto1 algorithm and discover that the random number generator is nothing but a 16-bit linear function. This was considered to be quite secured in 1994, but today with the fast multi-core processors in personal computers, this algorithm could be easily reversed with some basic understanding. To enhance the complexity, NXP asked for some time to come up with a solution to this problem with complex cryptographic functions and the result is MIFARE PLUS.

In this article we would know further what is MIFARE PLUS and how should a system based on MIFARE CLASSIC be migrated to MIFARE PLUS in different stages / levels. The key features of MIFARE PLUS that make systems more secured and faster than MIFARE Classic are:

- 7-byte UID instead of an old 4-byte UID
- Simple fixed memory structure backward compatible with MIFARE CLASSIC
- Usage of Advanced Encryption Standard (AES) instead of Crypto1: US Government approval for AES to be used on all secret documents beyond 2030
- True Random Number Generator (TRNG) tested against AIS 20
- Composite Common Criteria EAL 4+ certification for IC
- Freely configurable Access Conditions (Anti tear function for consistent deployment of changing keys and access conditions)
- Extra memory space to store the AES keys (A & B) for all sectors, instead of 48-bit keys
- Increased speed upto 848kbit/s, as against 106kbit/s
- Transmission security using CMAC (Cipher Message Authentication Code) as per NIST 800-38B
- Random UID, supporting anti-privacy features
- Write operations increased from 100K to 200K cycles
- Two variants: Standard (S) and eXpert (X), for simplified and full features sets
- eXpert (X) variant supports data encryption using AES keys, proximity checks to avoid relay attacks, faster transactions and support for Value block over Standard (S) variant.

So let's see what MIFARE PLUS has to offer us and how it secures us. So to incorporate all this features of MIFARE PLUS in the existing MIFARE CLASSIC system, a road path has been designed and prepared, but made available public for the first time via this newsletter. A simple equation to the solution says that the cards definitely need to be replaced, whereas the readers could be simply upgraded (for existing readers) or re-designed (for new projects).

In general, a Project Manager or Technical Officer has to follow a set of identified function points for MIFARE PLUS migration, while switching their projects. To know more on these function points, please write to us at support@advanide.com and we assure you of our fullest support required to migrate your projects.



The table below shows the different levels and the status / migration path of cards and readers, in each level.

Level	MIFARE Cards	MIFARE Readers	Explanation
Level 0	The project already has the MIFARE CLASSIC cards in the system, whereas the MIFARE PLUS cards can co-exist in the system.	No change	MIFARE PLUS card IC has AES keys as well as 48-bit keys as per MIFARE CLASSIC, so unless the AES keys are enabled, the MIFARE PLUS cards can co-exist and behave as MIFARE CLASSIC cards. The system as whole i.e., MIFARE PLUS cards, MIFARE CLASSIC cards and the readers behave as MIFARE CLASSIC System, and features of MIFARE PLUS remains un-utilized. All new cards being issued are MIFARE PLUS cards.
Level 1	The project already has the MIFARE CLASSIC cards in the system, but they would now be slowly removed from the system. The MIFARE PLUS cards are now going to dominate the system	Readers are now empowered using the MIFARE SAM AV2 (if the existing hardware supports external SAM, if not, then reader hardware has to be changed). Details on how to upgrade the readers is shown in next section of this article	Readers are empowered with MIFARE SAM AV2, which supports 48-bit key system as well as AES keys. They poll the card, differentiate them and accordingly run the application.
Level 2	MIFARE CLASSIC Cards are all removed / migrated from the system. All the cards are MIFARE PLUS with AES authentication. Also AES Keys are updated in the card using the anti-tearing feature. MIFARE PLUS Standard doesn't support the AES authentication and MIFARE Classic crypto support simultaneously, whereas MIFARE PLUS eXpert does.	Readers are now using a mandatory AES keys for authentication and no more usage of 48bit keys; however the data encryption is still done using Crypto1 algorithm (on MIFARE PLUS eXpert version only).	Tests of all applications, i.e., readers and embedded application along with backend, is a must before proceeding to Level 2. If tests are not conducted or partial tested products are introduced, the system may collapse. Also if any MIFARE CLASSIC card is still there in the field, they will not function resulting in end-users' grievances, which has to be pre-planned.
Level 3	Since this is for new installations, all cards are MIFARE PLUS with a mandatory AES authentication. In this level, apart from the mandatory AES authentication, the data is also encrypted using the AES keys and a full host of features on MIFARE PLUS eXpert version only. See list below.	All readers are pre-designed to handle the MIFARE PLUS authentication using AES, but no backward compatibility to support MIFARE Classic.	This level can be considered as 'an extension of LEVEL 2', where all the cards are now MIFARE PLUS and all the installed readers doesn't support MIFARE Classic OR 'Configurations for fresh installations'.

In Level 3 MIFARE PLUS eXpert version supports the following features, which MIFARE PLUS Standard version doesn't:

- Data Encryption with AES keys
- Full Virtual Card concept support
- Proximity Check (protection against Relay Attacks)
- Extra commands to transact faster
- Support for Value blocks

Upon close observation, the migration from MIFARE Classic to MIFARE PLUS at any Level requires an upgrade or replacement of the key component i.e., the reader. Most of the times, this is the only component which is prone to attacks, sabotage and raising false alarms for disclosing behavior. In this component migration process, we guide you on how to upgrade or replace the readers and with MIFARE PLUS around, what are the necessary components required in a reader.

A RFID reader normally consists of a micro-controller programmed with embedded application and an interface (protocol handling, command flow and data interpretation) to the Reader IC, supporting communication with the card. NXP's MFRC series Reader ICs has built in Crypto1 crypto functions, whereby the SAM is not mandatory for a reader to function. As mentioned in the beginning, there are 10 million RFID readers installed in the industry, most of them not provisioning a SAM. Keys to the cards in such a reader are stored either inside the reader IC or hardcoded into the embedded application residing onto the controller. This enhances a faster transaction time with auto-select of sectors and thereby authenticating them with the pre-stored keys. Both the methods of keys storage are not secured and this could be a disaster for the system.

There are three options or methods to upgrade the RFID reader hardware in this migration process. To get the detailed information on the upgrade options, please write to us at support@advanide.com.

We can definitely help you along with NXP, to resolve your queries with respect to migration of your systems from MIFARE Classic to MIFARE PLUS. Meanwhile, below is the list of all documents, libraries and tools that are available on request from NXP. Please write to us, and we will assist your further to get these documents, libraries and tools:

- On the MIFARE PLUS Card IC
 - Preliminary data sheet for MIFARE Plus MF1PLUSx0 Mainstream contactless smart card IC for fast and easy solution development
 - Release Note MIFARE Plus Waffle Packs Engineering Samples
- Reader libraries
 - MIFARE Plus RD701 (PEGODA) Reader Library Engineering Samples
 - User Manual MIFARE Plus RD701 (PEGODA) Reader Library Engineering Sample
 - MIFARE Plus RC52x Reader Library Engineering Samples
- Demo Software
 - MIFARE Plus PC Demo Software Suite '42' (Alpha Version) for Engineering Samples
 - MIFARE Plus PC Demo Software Suite '42' User Manual for Engineering Samples
- Security recommendations
 - MIFARE Plus Key Diversification - Application Note
- Documentation, libraries and software for MIFARE SAM AV2

***From the desk of Line Management:
Current Trends in RFID Industry***



Holger Winterhalter
Head of Line Management

Global Responsibility for contact based technology,
i.e. Controller, Memories



Gaby Mönig
Line Manager

Global Responsibility for contactless technology,
i.e. RFID Memories, Reader IC's

We work very close with our suppliers in order to have the newest products in AdvanIDe's portfolio. Additionally, we get a better understanding of the market and spread this information to our sales and customers, especially on products, trends, tenders / RFQs etc. Furthermore, we take care that our FAEs always get the right training from our suppliers in order to support you - as customer - on the latest technical standards. Distribution doesn't mean "box shifting" at all. Distribution means also dealing with information's and services. As an ID focused distributor, we see this as a "must" to provide our customers with dedicated information and service, especially on such fast moving markets like e-gov, banking and identification.

Market trend in Identification and Smart Card industry:

Overall, we observed a movement to identification products offering higher security. This means a development shift from simple memory applications with eventually read and/or right protection to secured crypto-controller solutions with open asynchronous algorithms and PKI. A very good example of this is the migration from MIFARE Classic 1k to MIFARE PLUS with AES cryptography, as explained in the article earlier.

The smart card industry has been continuously expanding with countries across the globe, identifying its true potential. The number of Smart card application projects has also been rising, demonstrating the versatility and robustness of the technology. The growing security needs, possible multiple usage and greater storage & processing capability are driving the growth of smart card industry world over and will also continue to do so in the future. The global shipment of smart cards surpassed an estimated 5 billion units in 2008 and this figure is projected to surge by nearly 12% through 2012.

The telecom sector is the biggest application market for smart cards, occupying more than 70% of the global smart card shipment in 2008. Growing number of mobile subscribers remain the largest contributor, driving sales of SIM cards worldwide. Use of smart cards in financial services sector has also been on rise buoyed by increasing use of Europay, MasterCard and Visa (EMV) standards. Increasing use of internet for making online payment transactions is also fueling growth in the global smart card industry as this technology enables consumers make secure and reliable transactions. Use of contactless smart cards in this regard has gained remarkable consideration and is forecasted to grow more than 30% through 2012. Besides this, the mass / rapid transport sector will experience the largest growth in usage of smart cards worldwide, nearly 25% in near future.

Partner Profile: **KSW Microtec AG**



ThinLam® by KSW

Source: KSW Microtec AG

KSW Microtec AG, with its headquarters in Germany, is the world's leading supplier of RFID (Radio Frequency Identification) components for applications such as Asset Tracking, Access Control & High Security, ePayment and eTicketing. KSW combines successful high-end wafer processing, extremely efficient assembly technology and far-reaching expertise in design. KSW has earned itself a leading position on the market as one of the most efficient, and simultaneously most flexible, producers of RFID components. The globally active company was founded in 1994 and has clean room production facilities in Germany. KSW is an investment holding of the listed venture capital company Deutsche Effecten- und Wechsel-Beteiligungsgesellschaft AG

headquartered in Jena.

KSW Microtec AG, offers high end customer specific RFID inlays and laminated transponders for eID documents already used in quantities of several millions in the US and Europe. The 2008 launched prelaminated Thinlam® achieves thicknesses down to 280µm and is extremely durable due to its patented chip connection technology. Compared to commercially available thicker products, the KSW Thinlam® offers whole new possibilities for manufacturing HF and UHF RFID cards and allows to implement security features using more layers for high value effects. The product can be manufactured based on 4 different materials: PVC, Polycarbonate, PET and Teslin®. KSW's Thinlam® sets new standards in quality and security for card manufacturing. The KSW polycarbonate based RFID Thinlams® can be easily laminated into polycarbonate cards, ensuring a matching material connection and thus preventing card delamination. As with other KSW products, the KSW polycarbonate tag can be produced in roll or sheet format, including customized sheet layouts. In-line testing and permanent process controls of the company's innovative technology ensure the highest quality standards are met, whether for high volume or customer-specific products.

To continue with innovation and quality on a high standard for our customers we need a strong partner who is able to work with us on such a high level, says Michael Schäfer (Director Procurement and Logistics). We consider AdvanIDe as such a strong partner especially with its high competence within the identification area. We can always trust on their fast logistical and technical support. AdvanIDe will continue to have an important strategic role as partner for KSW in the future.



*Thinlam can be delivered in 4 different materials
Source: KSW Microtec AG*

Future Trends in Smart Card Industry: From the Supplier's desk

LEGIC - Combining the worlds of logical and physical access on one single Smart Card Chip with LEGIC card-in-card solutions

LEGIC card-in-card solutions allow integrating applications on virtual LEGIC advant transponders into contactless or dual interface Smart Cards provided by third parties. This allows a combination of logical PC access and physical access control on one single Smart Card. This means, for example, that mobile phones can also operate as an access control credential, or credit cards be used as multi-functional membership cards.

Typical contactless multi-applications – such as physical access control, time and attendance or cashless payments – can be easily combined on a single chip with logical PC access or with credit cards, and extended as required. This further development in card-in-card technology will enable LEGIC to meet growing market demand for converged access solutions.

This flexible combination of contactless applications on any credential opens up a number of opportunities to combine the proven LEGIC applications with third party applications. Card-in-card technology can be transferred in no time onto any credential, including Smart Cards from third parties. Hybrid cards, which have both a contact-based and a contactless chip, are no longer needed.



Source: LEGIC Ident systems AG

The ability to integrate contactless applications in mobile phones or dual-interface cards opens up endless possibilities. As over 100 different applications are combinable such as e.g. access control or cashless payment applications. LEGIC card-in-card solutions offer great comfort and high security to end-users.

Fujitsu RFID chip using state-of-the-art Ferroelectric Memory technology

Fujitsu has successfully mastered the manufacturing know-how for the next generation high performance non-volatile memory using ferroelectric process technology. Fujitsu started mass production since 1999 and is now in our 10th year of supplying FRAM to the merchant market. Leveraging the inherent properties of FRAM such

as fast writing speed, high endurance and low power, Fujitsu has designed several RFID chips using FRAM. FRAM-based RFID has various prominent advantages over the conventional E2PROM-based RFID.

Fujitsu focuses on high performance and larger memory RFID which supports many read/write operations. Fujitsu's RFID chip will be suitable for applications such as portable data storage in addition of just being a simple ID code. More useful information can be read from the RFID directly without accessing to the back-end database system. For instance, meaningful information, product description, critical information like maintenance care, expiration date, etc. can be read off-line with a handheld reader.

FRAM has also exhibited strong tolerance to radiation. Its radiation hard properties has been independently tested and verified by various companies. This opens up a new array of applications like medical and pharmaceutical usage where radiation sterilization will be required.

Fujitsu RFID Product Offerings:

Part Number	MB89R119A	MB89R118B	MB97R8030 (New)
FRAM memory	256 Bytes (2048 bits)	2048 Bytes (16,384 bits)	2048 Bytes (16,384 bits)
User memory	232 Bytes	2000 Bytes	1664 Bytes
Carrier Frequency	13.56MHz	13.56MHz	860 ~ 960MHz
Standards	ISO/IEC 15693 ISO/IEC 18000-3 (mode 1)	ISO/IEC 15693 ISO/IEC 18000-3 (mode 1)	ISO18000-6C, EPC C1G 2
Data Retention	10 years	10 years	10 years
Endurance	10e10 times	10e10 times	10e10 times
Anti-collision	40 tags per second	30 tags per second	EPC Global standard
Anti-theft	EAS	EAS	EAS

Fujitsu has also implemented custom command above the ISO standard commands. It enables additional flexibility to data communications with the reader/writer. For example, Fujitsu's custom command can offer multiple block transfers for speed read or write to the large memory space in the chip.

The new MB97R8030 UHF class 1 Gen 2 chip is compliant to the EPC Global Gen 2 specification. However, it extends beyond the standard EPC product code to allow users to store up to 2000 bytes of information. An additional SPI interface offers an alternate means for accessing the FRAM from the usual radio interface.

LA Metro selects NXP's MIFARE Plus Microcontroller IC for Ticketing: Contactless TAP card will feature best-in-class security and easy upgrade capabilities

Eindhoven, The Netherlands, June 1, 2009 – NXP, the independent semiconductor company founded by Philips, today announced that Los Angeles County Metropolitan Transportation Authority (LA Metro) is the world's first transport operator to implement NXP's MIFARE Plus contactless technology for its automatic fare collection infrastructure. LA Metro, which already uses a MIFARE Classic-based system, is upgrading the Transit Access Pass, or TAP card, to include MIFARE Plus microcontroller smart card ICs. On an annual basis, LA Metro attracts approximately 480 million boardings in the Greater Los Angeles Area, and all passengers can enjoy convenient tap-and-go transport and a contactless ticketing system delivering advanced chip security features, provided by MIFARE Plus.*

"LA Metro's chief goal is to provide mass transit riders with a hassle-free traveling experience based on leading contactless technology that is both easy to use and robust," said Jane Matsumoto, Deputy Executive Officer, LA Metro. "Security is a key element of our system, and NXP's MIFARE Plus has proven to meet all our demands related to security features and superior scalability. With MIFARE Plus, LA Metro is implementing a transport ticketing system that provides outstanding convenience to our passengers, while also anticipating system security requirements for the future."

MIFARE Plus is the latest addition to NXP's market-leading MIFARE family of contactless technologies used in transport networks and access management worldwide. MIFARE Plus meets the highest industry standards in performance and security, including 128-bit Advanced Encryption Standard (AES) cryptology and an easy

migration path from existing MIFARE Classic infrastructures.

“Working with LA Metro in one of the most populated cities globally is a strong endorsement to the high standards NXP places on delivering leading contactless solutions to the market,” says Henri Ardevol, general manager, automatic fare collection, NXP Semiconductors. “In addition to its backwards compatibility into existing MIFARE systems, MIFARE Plus features open standards encryption in a very cost effective solution ideally suited for mass transit.”

Migration planning is made easier as MIFARE Plus supports the pre-issuance of new cards; coexistence of current and new cards; and software-based infrastructure upgrades. After upgrading the system infrastructure, service operators can easily switch MIFARE Plus-powered cards in the field to a higher security level without the need to revoke or re-issue the cards. MIFARE Plus contactless technology comprises a number of additional security and privacy features which, when used optimally in the infrastructure, provide a system that prevents individuals from being identified and tracked by others. It is targeted to receive Common Criteria EAL 4+ certification and complements NXP’s leading range of contactless technologies, such as MIFARE DESFire and SmartMX, which are already providing superior levels of performance and security in the automatic fare collection, access management, eGovernment and banking markets.

NXP MIFARE Plus is based on open global standards both for air interface and cryptographic methods. It is available in two versions: MIFARE Plus S, the Slim version, for straightforward migration of MIFARE Classic systems, and MIFARE Plus X, the eXpert version, which offers more flexibility to optimize the command flow for speed, privacy and confidentiality. MIFARE Plus X offers a rich feature set, including proximity checks against relay attacks.

MIFARE Plus is fully functional backwards compatible with MIFARE Classic 1K / 4K. Interoperability with MIFARE Classic has been verified by the independent MIFARE Certification Institute. MIFARE Plus offers the possibility to issue cards seamlessly into existing MIFARE Classic applications, before the infrastructure is upgraded. Once the security upgrades are in place, MIFARE Plus cards can be switched to a more secure mode in the field with no customer interaction necessary. AES (advanced encryption standard) is then being used for authentication, encryption and data integrity. MIFARE Plus supports high-speed communication between card and terminal at up to 848 kbps/s, for time critical services. The read range of up to 10 cm increases the convenience of the touch-and-go experience.

Security levels

A MIFARE Plus card supports one pre-personalization and 3 security levels. Cards operate in one security level at any given time and can only be switched to a higher level.

An automatic anti-tear mechanism is available for secure deployment of rolling keys. If a card is removed from the field during a key update, it either concludes the update or automatically falls back to the previous key. NXP recommends 7 Byte UID, but offers 4 B UID versions of MIFARE Plus during migration. MIFARE Plus is available in the proven MOA4 module and as sawn bumped wafers, no changes for existing manufacturing processes necessary.

For benchmark security on the reader side, the MIFARE SAM AV2 (secure application module) is available. The Common Criteria 5+ certified IC includes all MIFARE Plus commands, secure key storage and AES calculation for a reader device. To support the design-in process for reader manufacturers and solutions developers, NXP provides MIFARE Plus documentation, application notes, and software toolkits.

New Employees:

The following new employees have joined our team since our last newsletter:



In our Beijing, P.R. China office:

Brian Niu,
Regional Sales Director,
P.R. China
brian.niu@advanide.com.sg



Carlo Ng,
Sales Manager,
North China
carlo.ng@advanide.com.sg



In our Walluf, Germany office:

Frank Tekampe,
Regional Sales Director,
Europe & Africa
frank.tekampe@advanide.com



Oliver Stiegler,
Purchasing Officer
oliver.stiegler@advanide.com

Luck Draw Winners:

Amongst the new subscribers to our newsletter, we have drawn 3 lucky winners of a NOKIA 6212 NFC phone. The winners have been notified by email:

- *Mr. Quentin Peach from Taufkirchen in Germany*
- *Mr. Giriraj from Bharat Electronics Limited of Bangalore in India*
Mr. Giriraj is Manager of the Smart Card Group of Bharat Electronics Limited, a Govt. of India undertaking with Ministry of Defense. He has worked extensively on various e-Gov. projects involving the Multi-purpose National ID Card, Access Control Systems for the apex bank and biometric based monitoring system for the city municipal corporation, Mumbai
- *Mr. Sai Prasad from Digant Technologies of Bangalore in India*
Mr. Sai Prasad is CEO of Digant Technologies, who is our focused partner in designing and manufacturing of NFC modules and other RFID readers

Congratulations, you all will be receiving a NOKIA 6212 NFC Phone shortly!

