Payment
Product Portfolio

About ACE

ACE Product Portfolio

The acronym ACE stands for Austria Card's EMV smart card product lines that provide a wide set of EMV functionalities, according to both MasterCard Worldwide and Visa Inc. specifications.

Austria Card's ACE payment chip product portfolio is composed of native and Java Card product lines including both contact-based and dual interface product families.

The operating system is the heart of your smart cards. As we at Austria Card know that it is essential to have the right heart in the right place, we offer native as well as open operating systems.

ACOS, Austria Card's native operating system, is available for contact-based, contactless and dual interface solutions. ACOS forms a closed system and consequently offers extra security. Our in-house development team is flexible to your needs and provides customized applications and functionalities for your payment cards. All open systems contained in the payment product range guarantee absolute independence. Standardized applications ensure international compatibility and leave ample space for all kinds of adaptations.

ACE 2000 Product Line

Austria Card's ACOS operating system is the technological core of ACE 2000. The ACE product family is implemented on different microcontrollers to fulfil all varieties of market needs on the highest level of customer satisfaction and ensure state-of-the-art product security.

ACE 2000 Advanced

ACE 2000 Advanced stands for Austria Card's EMV 2000 compliant smart card high-end product range. Based on Austria Card's ACOS EMV operating system, ACE 2000 Advanced comprises a set of mandatory and optional EMV credit/debit functions in accordance to both Visa and MasterCard specifications including Dynamic Data Authentication (DDA) support. Security of offline transactions – both contactless and contact – is enriched by Combined DDA and Generate Application Cryptogram (CDA) processing.

In addition to the EMV 2000 functionality, ACE 2000 Advanced supports an on-card ISO/IEC 7816-4 file system with comprehensive security mechanisms for implementation of non-payment added-value customer applications. The on-card file system support is of particular interest for loyalty applications that could be placed on an ACE card in addition to the EMV core functionality.

ACE 2000 Advanced is available in 3 variations:

- ACE-M 2000 Advanced compliant to MasterCard M/Chip Advance specifications
- ACE-V 2000 Advanced compliant to Visa's VIS 1.5
- ACE-L 2000 Advanced for customer loyalty applications. ACE-L 2000 Advanced can be issued as stand-alone application or combined with either ACE-V 2000 Advanced or ACE-M 2000 Advanced.

ACE 2000 Advanced stands for DDA-capable contact-based products featuring not only the Dynamic Data Authentication (DDA) method but also the following core features as specified in the M/Chip and VIS specifications:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA and Application Cryptogram Generation (CDA)
- Card Risk Management Checks
- Cardholder Verification: Plain text or encrypted offline PIN
- Card-Issuer Authentication
- Issuer Script Processing
- Transaction log

Multi-Application Support

Both ACE-M 2000 Advanced and ACE-V 2000 Advanced allow creating as many EMV or loyalty applications on a card as is allowed by the available space in EEPROM. In other words, a number of applications that the card may hold are limited by available EEPROM only.

Any EMV application may share its PIN with one or more other applications.

Support for Loyalty Applications

To support implementation of loyalty applications, ACE-L 2000 Advanced offers the following:

- ISO/IEC 7816-4 file structures and commands
- Secure messaging
- Comprehensive file access control mechanism allowing implementation of complex access control polices

ACE 2000 Dual Interface

ACE 2000 Dual Interface stands for Austria Card's EMV compliant dual interface smart card product range. Based on Austria Card's ACOS EMV operating system, ACE 2000 Dual Interface supports contactless payment transactions and comprises a set of mandatory and optional EMV functions in accordance with both Visa (VIS 1.5 and VCPS 2.1) and MasterCard (M/Chip Advance Payment and Data Storage) specifications.

Security of offline transactions – both contactless and contact – is enriched by Combined DDA and Generate Application Cryptogram (CDA) processing.

In addition to the EMV 2000 functionality, ACE 2000 Dual Interface holds an on-card ISO/IEC 7816-4 file system with comprehensive security mechanisms for the implementation of non-payment added-value customer applications. The on-card file system support is of particular interest for loyalty applications that could be placed on an ACE card in addition to the EMV core functionality.

Being a high-end payment card, ACE 2000 Dual Interface may hold multiple contactless and contact-only EMV and ISO/IEC 7816 applications for payment, authentication, and customer-specific programs.

ACE 2000 Dual Interface is available in three variations:

- ACE-V 2000 Dual Interface compliant to Visa Contactless Payment Specification 2.1 and VIS 1.5
- ACE-M 2000 Dual Interface compliant to MasterCard M/Chip Advance Payment and Data Storage Specification

- ACE-L 2000 Dual Interface for customer add-on loyalty applications. ACE-L 2000 Dual Interface can be combined either with ACE-V 2000 Dual Interface or ACE-M 2000 Dual Interface.

Altogether, ACE 2000 Dual Interface features the following functions as specified in the M/Chip and VIS specifications:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA and Application Cryptogram Generation (CDA)
- Card Risk Management Checks
- Cardholder Verification: Plain text or encrypted offline PIN
- Card-Issuer Authentication
- Issuer Script Processing
- Transaction log

Multi-Application Support

Both ACE-M 2000 Dual Interface and ACE-V 2000 Dual Interface allow creating as many EMV applications on a card as the available space in non-volatile memory may allow. In other words, the number of applications the card may hold is limited by the available non-volatile memory only.

Any EMV application may share its PIN with one or more other applications.

Support for Loyalty Applications

To support the implementation of loyalty applications, ACE-L 2000 Advanced offers the following:

- ISO/IEC 7816-4 file structures and commands
- Secure messaging
- Comprehensive file access control mechanism allowing implementation of complex access control polices.

MIFARE® Classic Emulation

ACE 2000 Dual Interface offers a complete MIFARE classic emulation. In addition, access to the MIFARE memory area can be performed via a contact interface using ISO/IEC 7816-4 commands.

The MIFARE emulation uses memory, which is taken from the file system. The card can be configured to support either no MIFARE emulation, or 1K MIFARE Classic or 4K MIFARE Classic.

ACE AX Product Line

Austria Card provides ACE AX, thus offering a range of Java Card™ products. Our solution is based on independent, industry-wide, specifications provided by Oracle and the GlobalPlatform consortium.

The platform is compliant with relevant ISO standards and EMVCo specifications. The open nature of ACE AX enables the card issuer to load applications from different vendors, all written according to the same set of specifications: Oracle's Java Card specification and GlobalPlatform card specifications provide a powerful basis used across the industry for the design of smart card applications. These cards are interchangeable. ACE AX can replace almost any Java Card in existing infrastructures. By leveraging proven standards such as ISO/IEC 7816, Java Card or GlobalPlatform, the card is

interoperable with a wide range of systems and tools on the market and already in operational use. This allows the seamless integration of ACE AX into existing card infrastructures.

Java Card Features

Thanks to the open architecture of the Java operating system concept, cards are available from several vendors. Java applets can easily be loaded and they work on the entire Java Card range (appropriate hardware resources required).

As a true Java Card platform, ACE AX offers a fully-featured multi-application support:

- Multiple applications on one card (depending on EEPROM-size)
- Post-issuance loading of applications
- Wide range of software vendors for applet development
- Strict segregation of applications

Versions and Variations

ACE AX is available in a number of versions to support Visa and MasterCard EMV specifications over the contact and contactless interfaces:

- ACE-V Dual Interface AX compliant to Visa Contactless Payment Specification 2.1 and VIS 1.5
- ACE-M Dual Interface AX compliant to MasterCard's M/Chip Advance specifications
- ACE-V Advanced AX compliant to Visa's VIS 1.5 specifications
- ACE-M Advanced AX compliant to MasterCard's M/Chip specifications

MIFARE™ Classic, MIFARE Plus™, or DESFire™

ACE Dual Interface AX offers optionally MIFARE™ Classic, MIFARE Plus™, or DESFire™ emulation on-board.

ACE Features at a Glance

Millions of different card types are read every day at real and virtual points of sale. The future belongs to electronic payment – and to Austria Card's customers. One of the most important features of technological services is flexibility. ACE products are tailored to your individual needs and ensure utmost flexibility.

ACOS Native Product Lines

	ACE 2000 AIps	ACE 2000 Advanced	ACE 2000 Dual Interface
Platform	ACOS native	ACOS native	ACOS native
EEPROM Size	8 kByte	8 kByte	16 kByte
MasterCard EMV Specifications	M/Chip Advance *)	M/Chip Advance *)	M/Chip Advance *) and Data Storage
Visa EMV Specifications	VIS 1.5	VIS 1.5	VIS 1.5, VCPS 2.1
Authentication Methods	SDA	SDA/DDA/CDA	SDA/DDA/CDA
CAP/DPA Support	Yes	Yes	Yes
Multi-application support	Yes	Yes	Yes
EMV CPS Personalization Method	Yes	Yes	Yes
ISO/IEC 7816-4 and Austria Card Loyalty System support	Yes	Yes	Yes
MIFARE™ Classic	--	--	Yes

*) M/Chip 4 support through M/Chip 4 backward compatibility mode available in M/Chip Advance

ACE AX Product Lines

	ACE AX Advanced	ACE AX Dual Interface
Platform	Java Card	Java Card
EEPROM Size	12-40 kByte	12-80 kByte
MasterCard EMV Specifications	M/Chip 4 M/Chip Advance *)	M/Chip Advance *) and Data Storage
Visa EMV Specifications	VIS 1.5	VIS 1.5 VCPS 2.1
Discover EMV Specifications	D-PAS	D-PAS Contactless D-PAS
American Express EMV Specifications	AEIPS 4.2	AEIPS 4.2 and Expresspay 2.0
EMVCo Specifications	CPA	CPA
Authentication Methods	SDA/DDA	SDA/DDA
CAP/DPA Support	Yes	Yes
Multi-application support	Yes	Yes
EMV CPS Personalisation Method	Yes	Yes
MIFARE™ Classic, MIFARE Plus™, or DESFire™	--	Yes

For availability of particular ACE AX product configurations please contact your Austria Card sales representative.

*) M/Chip 4 support through M/Chip 4 backward compatibility mode available in M/Chip Advance

Contactless Expertise

Austria Card Offers FIDO®

Austria Card has added an additional layer of security and convenience by providing FIDO® certified cards and other form factors.
Passwords – even the most complex ones – are not sufficiently secure. Especially financial institutions push towards higher security solutions of authentication using secure hardware. To mitigate the risks of stolen passwords for all sorts of online accounts, the FIDO® includes a second authentication factor on a secure hardware.

The use of FIDO® technology transcends industry boundaries. Some application possibilities include:

- Financial services
- Online Banking
- E-government
- M-commerce
- Cloud storage
- E-Mail accounts and social networks
- Medical services

Austria Card's FIDO® Products

FIDO® U2F-application already runs on ACOS, Austria Card's native operating system. ACOS FIDO® has passed the FIDO® interoperability testing, and Austria Card can thus offer to its clients FIDO® certified products. Austria Card is the first member of the alliance that has a certificate for its FIDO® implementation on EMV payment products i.e. payment smart cards. Austria Card offers the following form factors:

- Dual Interface smart cards
- Contactless smart cards
- Mobile stickers
- Key fobs
- Wristbands and watches

Multiple Advantages

All options for this two-factor authentication are strongly resistant to phishing, but the use of a contactless credit or debit card has multiple advantages. First, everyone owns a smart card. Second, people tend to carry their cards in their pockets wherever they go. And there's a major benefit for the issuers as well: The visibility of their cards and thus their logo increases exponentially. The bank's logo is seen every time customers logs into their e-mail, social media, or other accounts.

Moreover, Austria Card can also offer a FIDO® Authentication Server Solution that includes:

- Easy integration / smart interface to CMS
- Token management
- Independent channel for token communication
- Support for mobile devices
- Reference implementation
- Integration support

Background

In order to reduce sole reliance on passwords, the FIDO® Alliance members share technology and collaborate to develop open specifications for universally strong authentication. The goal is to create authentication methods which are interoperable, more secure and private, and easier to use – giving the possibility to cover as many services as possible with a single device. Since its launch in 2013, the FIDO® Alliance has grown beyond 200 companies and government agencies.

ACE Payment Gear

The ACE Wearables are the perfect complement payment tools. They include form factors such as key fobs, wristbands, pendants, or even plush mascots.

The items of this product line are certified by MasterCard, and payment is possible at every contactless terminal.

Austria Card uses the latest chip generation for its payment wearables, so that multiple applications such as loyalty, ticketing, or access authorization are possible with only one item. So not only banks, but also public transport operators and retailers can profit from the product. Additionally, companies across industries can partner together and thus enhance their visibility and market share.

ACE Wearables can run the following applications:

- M/Chip Advance
- ISO/IEC 7816-4
- Mifare Classic

Fully-fledged Banking Card

The ACE Payment Gear items function as fully-fledged contactless credit- or debit cards. Like your customer's banking cards, they are linked to their bank accounts and can be used at every contactless POS terminal worldwide.

Usage at Special Events

Ace Payment Gear offers great application possibilities at special events such as festivals or football games. Whether you introduce the gadgets as an add-on to reward your most loyal customers (such as football fans with a yearly subscription) or as an opportunity to attract new ones, is completely up to you. Sponsoring or partnering with event organizers also gets easier - simply make your visitors pay with the flick of their wrist or with their key fob.
Your customers have the benefit of paying without even opening their wallets and don't need a PIN-code verification for small transactions. Purchasing has never been so easy!

Display your Brand

Our payment wearables are completely customizable. You have constant brand visibility even when your customers' wallets stay closed. Every time your customer jangles his key fob, your brand becomes visible, immediately sparking discussion about the innovative product.

Reach New Target Audiences

The ACE Payment Gear represents a suitable accessory product to the bank's card portfolio and is appreciated particularly by younger client segments. Give them a payment instrument tailored to their needs!

ACE Mobile Tag

Ready to be attached to any mobile phone, the ACE Mobile Tag is the ideal alternative or complement to contactless cards.

A special shielding layer ensures reliable performance on various housings or surfaces.

In addition to contactless payment, other applications such as loyalty programs, ticketing, or access authorization can be integrated.

Advantages of the Sticker:

The ACE Mobile Tag offers a wide range of benefits including:

- Flexibility: Perfect adhesion even to multiple surfaces, including irregular ones
- Thinness: The sticker is extremely thin and can be placed inside the housing of suitable mobile phones if desired.
- Convenience: Easy to attach, easy to use.
- Attractiveness: High-grade appeal due to leading-edge printing techniques.
- Ubiquity: Sticker operates on any object.
- Reliability: Certified security and quality (DIN/ISO 9001, NASPO)

Personalisation

The ACE Mobile Tag is placed on an ID-1 shuttle card enabling optical and contactless personalization and insertion of tags with standard machinery.

Tag Specification	
Applications	M/Chip Advance; ISO/IEC 7816-4; Mifare Classic
Dimension	40 x 35 mm
Overall Thickness**	Approx. 550 µm
Top Laminate	PET, transparent, glossy surface (matte available upon request)
Printing	Digital 4 colour print
Optical Personalisation	Thermo print, laser engraving
Temperature Range	- 25 to 60 °C

**) without chip

Shuttle Card Specification	
Applications	ID - 1
Material	PVC
Printing Options	1c or 4c
Design Options	PVC card design options upon request

Mobile Payment

Mobile NFC-Services for Payment

The Promise of Convenience

Consumers want a smooth, fast, and easy payment experience, one that is in line with their everyday use of technology. When they come to the cash register to pay for their meal or purchases, many can now simply hold up their mobile phones instead of handing over bills or pulling out a credit card. At the same time, Austria Card clients and their end-customers can rest assured that they have the same high security standards as they are used to from our other products. These are some of the benefits of Austria Card's mobile payments solutions that your customers will enjoy:

- Ubiquity of smartphones
- All over the world massive rollouts of contactless terminals
- Speed of transaction
- No need to pull out the wallet
- No need to insert the card
- No PIN-necessary for small value transactions, thus even faster payment process
- See and store the payment history
- Integration with mobile wallets and loyalty programs
- Highest security standards in line with the specifications of the credit card companies

Mobile Payment is Gaining Pace Worldwide

The unprecedented promise of speed and convenience of mobile payment creates new opportunities to drive the volume of non-cash payments. Contactless infrastructure is rising all over the world, thus enabling the ascent of payments via the smartphone. Austria Card has been one of the pioneers in this technology and acts as a Trusted Service Manager (TSM), which is the major security component in the complex NFC ecosystem.

Mobile NFC-Services

By utilising Near Field Communication (NFC), the mobile phone becomes a fast and convenient means of payment. Furthermore, NFC offers additional functionalities:

- Contactless payment at the point of sale
- Purchase of e-tickets
- Access control to restricted areas
- Payment history
- Bonus points
- Loyalty campaigns

A secure element within the mobile phone holds all sensitive information related to these functionalities in order to ensure the highest security standards. One major advantage of mobile payments for financial institutions is the user interface capability, which can be utilized for various kinds of marketing purposes. For the development and customisation of smart phone applications, payment schemes' specifications and best practice guidelines are already available.

Trusted Service Manger

A TSM acts as a broker between the various service providers and connects with the mobile network operators. Furthermore, the TSM is an important provider of technology and manages the mobile applications.

Cloud-Based Payment Solutions and Wallets

HCE - No Need for a Secure Element

Host Card Emulation (HCE) is an alternative to the conventional NFC-payment technology. Using HCE, the payment application resides on the phone's operating system (instead of in the physical secure element), and it directly interacts with a secure cloud system and the NFC-controller. Thus, there is no need for a card issuer to use SIM or other secure elements for contactless NFC-transactions.

HCE assumes that any data stored on a handset is vulnerable and therefore restricts the storage of sensitive data to host or "cloud" databases. These databases must be managed to a high security standard. The security requirements are a very high level, exceeding common security (e.g. PCI DSS) and equivalent to card personalization bureaus. Preventing unauthorized access in HCE depends on four pillars: limited use keys, tokens, device fingerprinting, and transaction risk analysis.

HCE is endorsed by Visa and MasterCard. Google has made HCE-technology available on its Android operating system. Any Android 4.4 device equipped with HCE-technology can emulate an NFC-smart card and support payments, loyalty programs, card access, and transit passes.

Mobile Wallet - A Convenient Payment Method

The Mobile Wallet is a mobile payment service based on NFC-technology. Using the wallet consumers can pay by just tapping the mobile phone on the payment terminal. This automatic payment mode immediately accepts low-value payment transactions without any further confirmation.

User Payment Control

Depending on the type of mobile wallet in use, a high-value payment needs to be authenticated by the end-customer on the mobile phone or the payment terminal. Different payment properties such as the kinds of cardholder verifications (Mobile PIN, PassCode, online PIN, security patterns) can be defined by the issuer.

Benefits of the Mobile Wallet

- Mobile payment with multiple cards combined in just one app
- Convergence of different categories such as payment, loyalty, access, etc.
- New content items can be added through the marketplace
- Easy handling
- Instant activation and delivery of service content
- Enhanced user experience by new functionalities such as displaying the transaction history

Payment History

In addition to managing and controlling the wallet´s payment behaviour the consumer has access to a detailed transaction history, including information on the amount, merchant, location, and time of a transaction.
On top of that, various other control features such as visualisation of a spending history subject to merchant categories are available.

Services and Tools

ACE Pin over SMS

Cardholders no longer have to wait for the postal delivery of their payment card PIN mailer. Austria Card provides PIN over SMS.

Approaching New Technology

Austria Card developed a flexible and secure PIN distribution solution using the standard and globally available Short Message Service (SMS) technology.

The SMS gateway is hosted by Austria Card and can be connected directly to either national Mobile Network Operators or SMS Mass Aggregators.

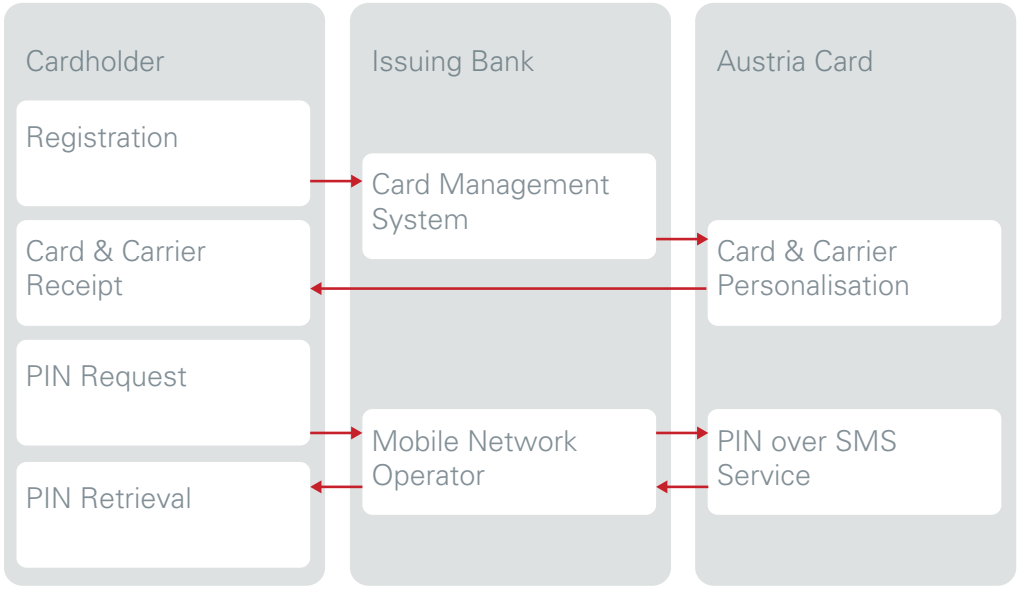
Benefits

- Profitability by replacement of additional PIN mailer printing and courier service
- Environmentally friendly
- Strong security using two factor authentication
- High availability service
- Easy handling
- Instant cardholder PIN access for card usage

Just One Number Away

To obtain all profits and benefits of PIN over SMS service, the data interface between the issuing bank and Austria Card only has to be extended with the mobile telephone number of the cardholder. The process is simple and time-efficient, while at the same time guaranteeing data protection across all stages.

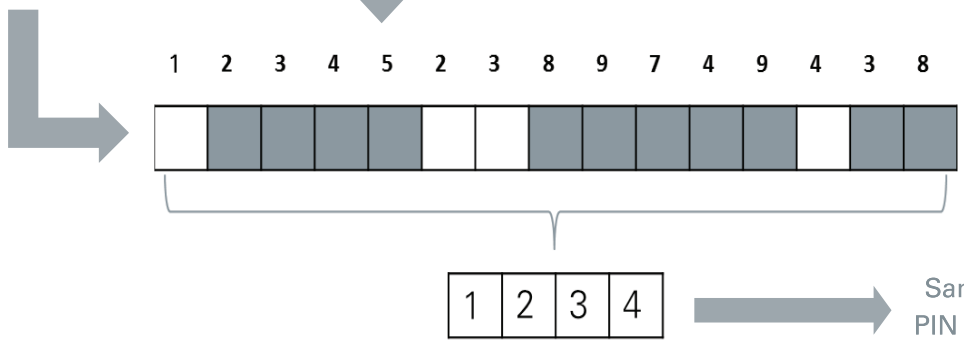
PIN over SMS Workflow



Austria Card's data management system is taking care of the processing of all relevant information necessary to enable secure PIN value distribution via the SMS gateway directly to cardholders. This procedure saves money for the PIN issuer and time.

Requesting the PIN Value

- On the card carrier, the cardholder is instructed to send the personalised and unique identification number to the Austria Card SMS gateway.
- A unique identification number contains a security check digit to prevent typing errors on the cardholder's side
- The actual PIN is not initially transmitted to the registered mobile number – the cardholder has to trigger the process
- The sensitive PIN is securely delivered and securely stored on the mobile handset

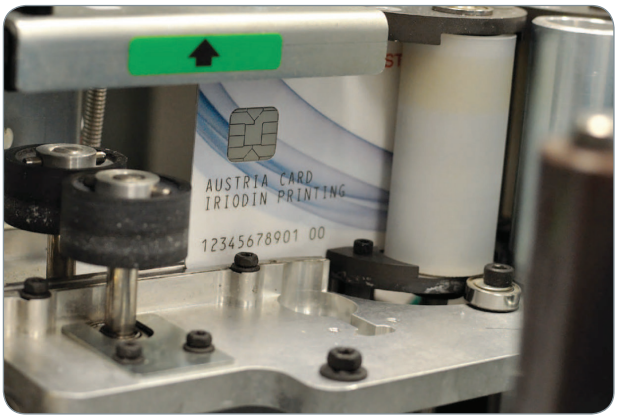


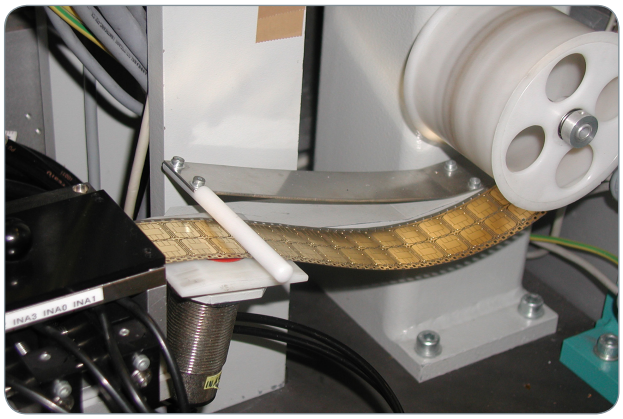
Features

Several features, so called "issuer specific security policies", can be defined per product:

- Reminder messages to the cardholder
- Fallback to carbon PIN mailer
- Forced fallback, initiated actively by the bank's Card Management System
- Denial-of-Service attack detection and blocking
- Extensive and automated report mechanisms
- Dynamic and multi-language SMS text
- Usage of different network operators based on their availability
- Support of prepaid cards
- Flexible system design allows fast and easy parameterisation of specific customer needs.
- Sensitive and security related processes are performed by certified Hardware Security Modules (HSM).

Card Personalisation





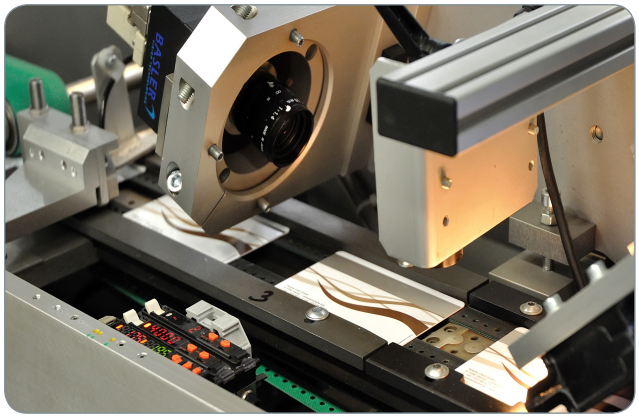
Austria Card – Personalisation Experts

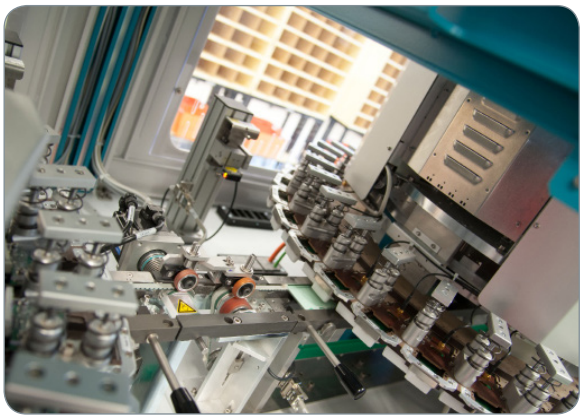
The characteristics

- More than 20 years of experience in personalisation
- More than 200 mio. cards personalised in Austria Card's personalisation centres
- Five personalization bureaus in Athens, Bucharest, Istanbul, Krakow, and Vienna add up to an unrivalled distribution network in the CEE region. With a homogenous infrastructure in place, all centres serve as mutual backups. This ensures optimized delivery capacity, distribution channels, and short lead times.
- To offer impeccable customers support, Austria Card has sales offices in Albania, Austria, Azerbaijan, Croatia, Greece, Jordan, Poland, Serbia, Romania, and Ukraine
- Fast reaction times
- Personalisation premises certified by Visa International, MasterCard® Worldwide, and Diners Club
- A ready-to-use personalisation solution for the ACE product line. This solution is as follows:
  - Based on the datacard SCPM or APM architecture
  - Also available for other hardware and software personalisation platforms, implemented by a variety of Austria Card partners

Three different types of personalisation

- The all-in-one desktop card personalisation solution is a full service provided by Austria Ca de and includes the following:
  - Chip personalisation, as well as software modules
  - Data management system
  - Carrier printing
  - Support for a number of desktop personalisation machines
- The chip personalisation consits of the following:
  - Personalisation software modules
  - EMV data preparation services and consulting
  - Personalisation test tools
- Magnetic stripe encoding
- The optical personalisation is made up of techniques for visible personalisation:
  - Embossing
  - Indent Printing
  - Laser Engraving
  - Thermo Printing
  - Custom Card Printing
- Lettershop fulfilment (incl. customised carrier letter, envelopes and attachments): Many of the carrier and advertising material is printed on Inform Lykos premises, which leads to shorter response times in many regions, especially the CEE area.
- PIN mailer print
- Direct mailing to the cardholder





Austria Card offers a set of ready-to-use applications to enable ACE personalisation in the most common chip personalisation environments. It goes without saying that all II ACE product lines are supported in the personalization process:

- ACE 2000 Alps
- ACE 2000 Advanced / ACE Advanced AX
- ACE 2000 Dual Interface / ACE Dual Interface AX

ACE personalisation applications are available off-the-shelf for two personalisation infrastructures:

- Datacard infrastructure
- Mühlbauer infrastructure

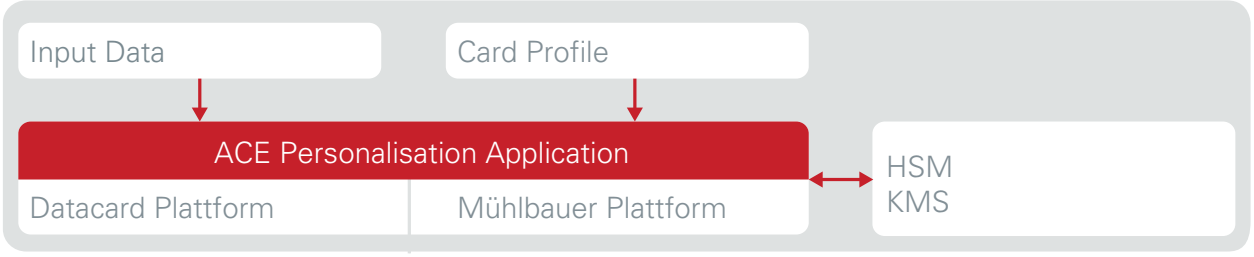
ACE personalisation applications for other hardware and software personalisation platforms are implemented by and available from a variety of Austria Card partners. As in other areas, our partner network helps us to provide a holistic service for our clients, where they benefit from having one single point of contact.

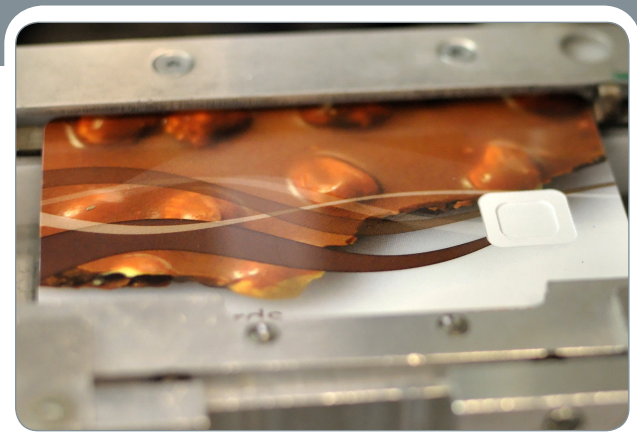
Mühlbauer Infrastructure

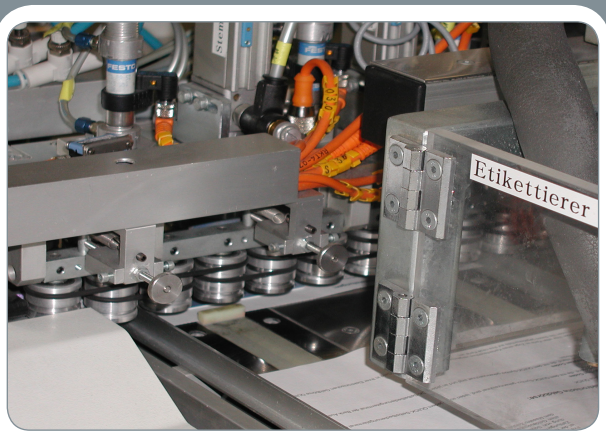
The ACE personalisation solution used in a Mühlbauer infrastructure requires at least the following components:

- Mühlbauer personalisation systems
- MCES
- Key database (Austria Card Key Server)
- ACE Crypto Unit, Thales HSM
- Input data loader (to load personalisation data into the machine database)

ACE Personalisation Infrastructure







Datacard Infrastructure

ACE Personalisation solution for a Datacard infrastructure requires at least the following components:

- Smart Card Personalisation Manager (SCPM)
- Datacard
- Object Server (key database)
- ID Works
- ACE Crypto Unit, Thales HSM

Austria Card ACE Personalisation Application

The personalisation software that was developed by Austria Card is an application implemented as a plug-in DLL, which is connected to the Datacard SCPM/ APM core or Mühlbauer MCES.
The ACE Personalisation DLL processes application-specific personalisation data, manages the HSM and then creates respective personalisation commands according to the card profile specification.

Card Profile

Austria Card's ACE Personalisation DLL uses card profiles as a static input to enable plausibility and seucrity checks and to define a structure of the data elements within the chip data block of the personalisation input file. It also defines necessary key translations during the personalisation.

Hardware Security Module

Hardware Security Modules (HSM) ensure the integrity and confidentiality of security-sensitive
personalisation data, e.g. cryptographic keys and PIN.

Key Management System

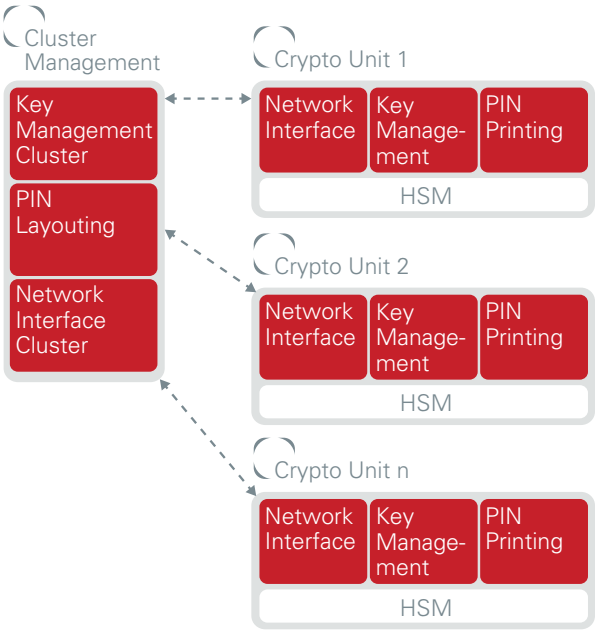
All cryptographic keys are stored encrypted in the Key Management System (KMS). Either the Datacard General Object Loader or the Austria Card Key Server can be used as KMS.

Affina One Step – Data Generation & Personalisation

Affina One Step is a personalisation solution provided by Datacard comprising both EMV data preparation and personalisation of smart cards inline.
Instead of using ACE Personalisation DLL, Affina One Step uses a Global Platform scripting engine, which is called Affina Profiles and Scripting. Austria Card provides Global Platform scripts to personalise ACE 2000 and ACE AX products supporting inline EMV data preparation.

ACE Crypto Unit

ACE Crypto Unit is a turnkey Hardware Security Module, which is specifically designed for EMV card issuing and secure PIN printing. Based on a FIPS 140-2 Level 3 certified plug-in board, ACE Crypto Unit provides a graphical user interface (GUI) for key management (KMS), PIN mailer layouting, and PIN mailer printing (PIN Printing Utility).
A redundant high speed network interface ensures a straight forward integration into heterogeneous personalisation area networks. The security concept of the system is compliant to the security requirements of payment schemes and PCI Card Production.



Key Management System

The Key Management System is GUI based and assures a convenient way to generate, export, import and delete keys or certificates. Besides symmetric key management, like 3DES and AES, the KMS also supports the management of asymmetric keys such as RSA and the Elliptic Curve.
In order to ensure compliance with all major payment schemes, besides a console or printer (only for export), a dedicated user management supports the import and export of keys components.

PIN Printing Utility

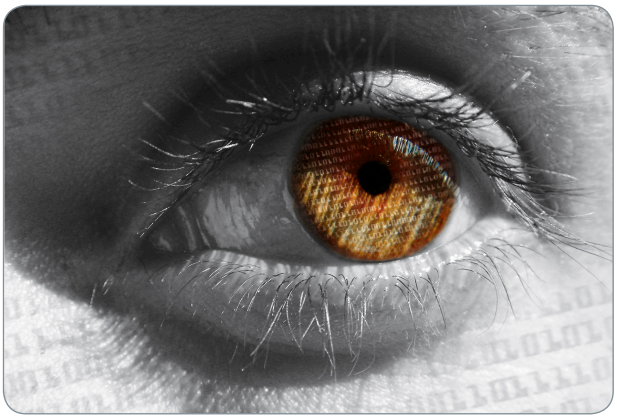
The PIN Printing Utility offers the possibility to print PIN mailers on either dot matrix printers or laser printers. Beside the PIN and the shipping address, the system allows for the printing of dynamic text modules and graphics. Colour printing is also possible, depending on printer hardware.
The included WYSIWYG layouting software allows for the designing of PIN mailers in a very fast and convenient way.

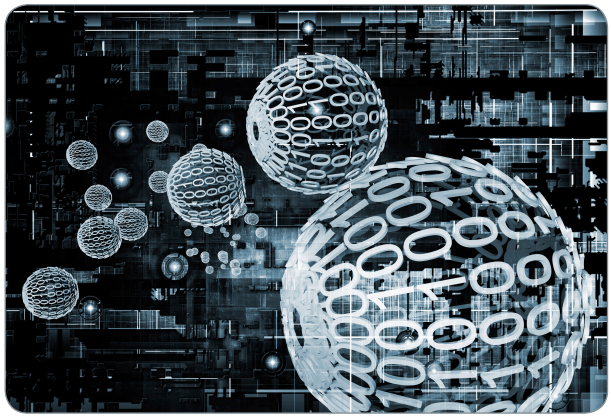
Network Interface

ACE Crypto Unit can be attached to standard Ethernet networks and uses redundant network interface cards to communicate with software clients.
Thanks to the open software design, the interface can be adapted to customer needs and is completely independent from the operating system. The communication between software clients and ACE Crypto Unit is encrypted by default.

ACE Crypto Cluster

Several ACE Crypto Units can be connected to ACE Crypto Cluster. A load balancing mechanism distributes the tasks to the units inside a cluster and also provides a fail-safe mechanism. The Key Management System automatically distributes all keys to all units within a cluster.





HSM Features

- Symmetric Algorithms
  - DES, DES2, DES3
  - AES
  - Modes: ECB, CBC
- Asymmetric Algorithms
  - RSA (up to 4096 bit)
  - DSA
  - ECDSA (up to 512 bit)
- Hashing Algorithms
  - MD2,
  - MD5
  - SHA-1
  - SHA-256
  - SHA-384
  - SHA-512
- Message Authentication Codes
  - SHA-1
  - SHA-256
  - SHA-384
  - SHA-512
  - MD2
  - AES MAC
  - DES/DES3 MAC
  - DES3 Retail MA
- Random Number Generation
  - DSA (512-1024)
  - RSA
  - ECDSA
  - PKCS#11 v1.5

Key Management Functions

- Key import (import of key components supported)
- Key export
- Generate (generation in components supported)
- Key delete
- Rich logging functionality (characterized by the fact that every key management operation is logged)
- Key backup

Operational Functions

- Encrypt
- Decrypt
- Sign
- Verify
- Translate key
- Derive key
- Generate CVV
- Generate PIN
- Translate PIN
- Generate PVV

Host System Features

- Usual in trade x64 server
- Microsoft Windows Server 2008 R2 operating system
- Microsoft SQL Server 2008
- TLS secured communication

Post-Processing and Data Output

Due to a flexible post-processing mechanism, the generated data can be manipulated before output. The data can either be written to a file, or stored inside ACE database for further processing.

Supported Applications

- Visa (up to version 1.5)
- MasterCard® (up to MChip Advanced)
- Diners DPAS
- Due to the flexible design, other applications can be implemented quickly and seamlessly based on the respective customers' demand

Supported Chip Platforms

- ACE Chip Platforms
- Global Platform
- EMV

Supported File Formats

- Card Personalisation Specification (CPS)
- Datacard Gen2E (TLV)
- Customer defined (flexible pre- and post-processing of files)

Supported Operating Systems

- Microsoft Windows XP, Vista, 7, Server 2003, Server 2008, Server 2008 R2; both 32 bit and 64 bit
- In addition, ACE Genesis Core access over other operating systems is optional, but not mandatory

EMV Triple Interface Personalisation Tester

The EMV Triple Interface Personalisation Tester (TPT) is a tool to ensure the logical validity of personalised EMV cards. It tests issuer data, optional loyalty applications and the congruence between all data stored on a card.

- Support of contact, Dual Interface and contactless cards
- MasterCard® *PayPass*™ and Visa payWave™ support

Test Tool for EMV SDA/DDA/CDA Cards

The following tests are implemented according to EMV 2000 v. 4.43:

- Correlation between magnetic stripe data and EMV smart card data
- Offline SDA/DDA/CDA-tests
  - Application selection
  - PSE selection
  - Initiate application processing
  - Read application data
  - Offline data authentication
  - Offline plain PIN verification
  - Offline encrypted PIN verification
  - CVV support
  - Visa VLP transaction
- Test of multi-application cards

Strictly Hierarchical User Concept

The EMV-TPT provides a multi-user concept to map all prevalent roles of industrial personalisation processes.

- Manager: test set-up
  - Maintenance of CA public keys
  - Maintenance of issuer master keys
  - Definition of test scenarios
  - Set-up of terminal data
  - Implementation of tests
- Developer: All features of the Manager plus extended debug logging
- Operator: Execution of tests only

Contactless EMV Transactions

- M/Chip Advance
- MasterCard *PayPass*™ M/Chip
- MasterCard *PayPass*™ Mag Stripe
- Visa MSD
- Visa qVSDC
- Visa contactless VSDC

Simulation of Issuer Host

The simulated issuer host generates issuer scripts, verifies cryptograms returned by the card and produces cryptograms for issuer authentication.

- Input mask for issuer master keys Derivation of card-specific or session keys
- Selection of issuer scripts MAC generation for issuer scripts Message encryption for issuer scripts
  - Application Block andUnblock
  - PIN Unblock, PIN Change, PUT Data
  - Update Record
  - Update EF-CRM (M/Chip Lite 2.1)
  - TC and ARQC validation
- ARPC generation
- Simulation of Authorization Request Codes
- VSDC+ (Issuer Discretionary Data)

Technical Data

The EMV Personalisation Tester can be connected to a Windows PC using an USB or TCP/IP interface. The offline EMV Personalisation Tester contains:

- Hybrid motor-move-in card reader for
  - Magnetic stripe
  - Contact chip and contactless chip
- Power supply (prim.: 100–240 V~, 50/60 Hz)
- Complete installation software
- Documentation
- Cabling

Congruence of Magnetic Stripe and Chip Data

The EMV-TPT retrieves magnetic stripe and chip data from the card. It performs analyses and a comparison with all corresponding smart card data objects.

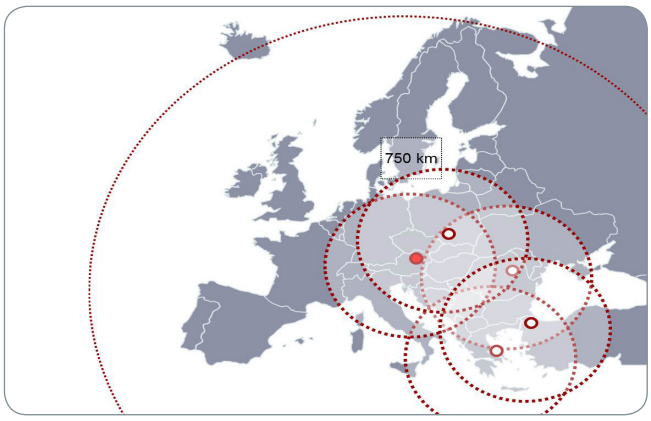
Support of Multi-Applications

Smart cards can contain EMV applications and/or non-payment functionalities and/or a customer individual application code. The EMV-TPT covers all combinations.

Analysis Display

The EMV-TPT produces test analysis output

- in tree views for easy interpretation by untrained users
- in a detailed EMV transaction trace for expert analysis



Austria Card is a market leading and internationally operating company in the field of secure communications for Payment, Government and Industrial applications. Since the introduction of chip-based payment cards in 1995, Austria Card has been a pioneer in the field of smart payment systems.

The development of the native operating system for smart cards (ACOS) in Austria Card's in-house Research and Development Department is one of the key components for today's success: ACOS complies with the global EMV standards and leaves ample space for flexible solutions to individual customer requests.

Being an expert in personalisation as well as data processing, Austria Card, as a long-time card manufacturer, has leveraged its experience and knowledge to offer products and services for and beyond smart cards: Austria Card is always exploring the latest technologies and, therefore, is able to utilise the newest mobile NFC trends by offering a professional TSM service: ACE SEM (ACE Secure Element Management).

In 2008, Austria Card became a member of one of the longest running successful company groups in Europe, LYKOS. The Group, which traces its roots back to 1897, develops, produces and personalizes smart cards for banks and the public sector.

Our personalisation centres are located in:

Austria
Austria Card-Plastikkarten und Ausweissysteme
Lamezanstrasse 4-8
1230 Vienna
T +43 1 610 65-0 | F +43 1 610 65-0
sales@austriacard.at

Greece
Inform P. Lykos S.A.
5th klm Varis-Koropiou
194 00 Koropi, Athens
T +30 21 066 97 800 | F + 30 210 66 29 536
sales@lykos.gr

Poland
Austria Card Polska Sp. z o.o
Warsaw Financial Centre
53 Emilii Plater St, 10th floor
00-113 Warsaw
T +48 22 528 67 77 | F +48 22 528 67 01
biuro@austriacard.pl

Romania
Austria Card S.R.L.
Soseaua Odai, no 347-363, Sector 1
013604 Bucharest
T+40 21 408 4545 | F +40 21 372 251 725
sales@austriacard.ro

Turkey
AUSTRIA CARD TURKEY KART OPERASYONLARI A.Ş.
İkitelli Organize Sanayi Bölgesi
Atatürk Bulvarı Deposite İş Merkezi
A6 Blok K:2 No:209 Başakşehir- İstanbul
T : + 90 (212) 4070019 F : +90 (212) 4070098

AUSTRIACARD

Information & Contact
1230 Vienna, Austria |
Lamezanstrasse 4-8
T +43 1 610 65-0 | F +43 1 610 65-0
sales@austriacard.at

www.austriacardag.com