eTicketing in public transportation

SAM-Server

Security in eTicketing

worldline
e-payment services

an atos company

Security, reliability and performance for electronic ticketing through use of the Worldline SAM-Server

Many transport companies in the public sector are (or will be) implementing the change from paper tickets to electronic tickets. One significant success factor with electronic tickets (eTicket) is the security of the whole system and the customers' trust in that security. The public sensitivity to topics such as confidentiality of personal data and protection against data theft is extremely high. Furthermore, due to an increased expansion and usage of eTickets, the future amount and complexity of transferred data will strongly increase. Because these data transfers are secured cryptographically as a matter of principle, topics such as throughput and response times will acquire a more significant meaning, i.e. performance and reliability of the security components have to be adapted to the load of the whole system.

Challenge

In addition to the general data protection requirements of using electronic tickets, operators of eTicket systems have to consider **security aspects** as well. Because an eTicket system is a large, distributed IT system, with many participating partners, a manipulation-free, high-availability operation has to be ensured. Possible attacks include:

- **Manipulation** of the data on the user smart card (e.g. changing single ride tickets to monthly tickets).
- Creating new entitlements on the chip-card, without involving a background system.
- **Altering** the data transferred to the product managers (e.g. the sale of 10,000 entitlements instead of 1,000) in order to generate higher billing figures.
- **Re-using** old data, in order to generate unjustified billing.

Guaranteeing security and preventing these scenarios are important requirements for the economic success of running an eTicket system.

Concept

The standard eTicket systems in Europe (ITSO, VDV-KA, Calypso) are supported by the ISO 14443 standard for NFC. For these chip-cards, the semi-conductor industry offers so-called SAM modules, which can be installed in public transport terminals, as a contact device. These SAMs (Secure Access Module) are cryptography devices in the form factor of a mobile phone SIM card, which **store keys in a non-readable form** and perform cryptographic operations. As long as there is only low load (or single transactions) at the end device (ticket terminals, control devices etc.), these SAMs readily fulfil the performance requirements. These SAMs have supporting processes and adapted software that reflect the specific requirements of the eTicket systems, personalisation for the operator and key management.

Specifically in the VDV Core Application (KA), the cryptographic processes are not restricted to single transactions (e.g. also batch operations):

- **Securing data exchange** between partners in an eTicket system association
- **Ticket purchase** using a card reader at the PC
- **Personalisation** of chip-cards during creation
- Creation of **printable paper tickets, with 2D Barcodes** (e.g. train tickets)

All these processes use cryptographic methods, whether signing exchanged data, or protecting transport keys during personalisation. Specifically, asymmetric encryption methods are very processor intensive and quickly cause performance problems when executed on the chip-card. In response to this challenge, there is a solution currently available in which a large number of SAMs are clustered, in order to provide higher cryptographic performance. However, these systems have stability problems and are expensive to manage.

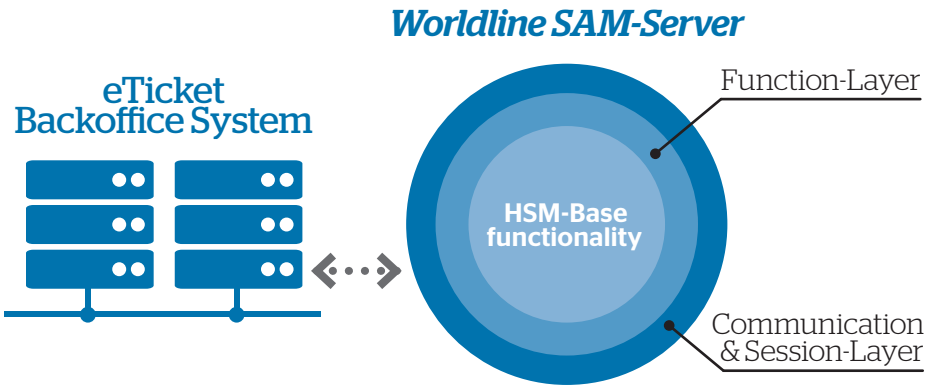
SAM Functionality in the Worldline HSM

Innovative Solution

Worldline offers a completely **new concept** for this problem. Worldline's own HSMs (Hardware Security Modules) were created, based on **many years' experience** in electronic payment. These are **high-performance, extremely secure cryptography computers**, specifically designed to adopt the role of securing electronic payment transactions. The **complete know-how** of both hardware and software is available at Worldline. **All relevant security accreditations** are available and furthermore, are in use at Visa and Mastercard and are endorsed by the German Banking Industry Committee. In order to enable the usage in eTicket systems, Worldline is currently developing a VDV-KA conform software, which will provide SAM compatibility to the HSMs.

The HSM portfolio includes a full software suite, which supports and implements the following functionality in the HSM:

- Scalability
- Redundance
- Key Management

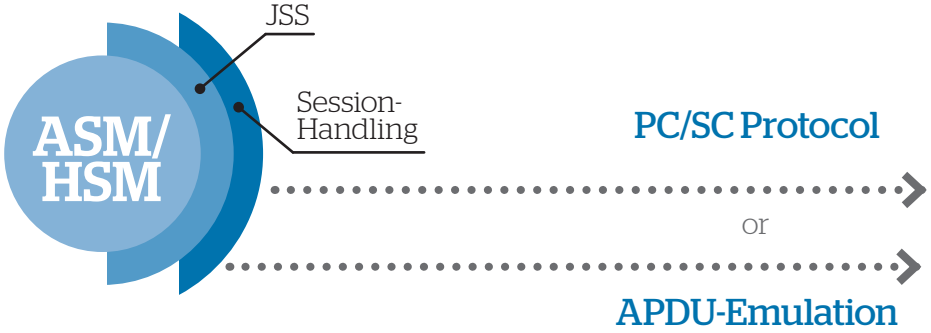


Layout of the Worldline HSM Solution

Advantages for the operator

Deployment of the Worldline HSM brings several advantages for the operator. Of special importance is the **very fast processing** - creating a signature in the HSM takes just a few milliseconds, as opposed to a SAM, which takes several tenths of a second. As a direct consequence, the **system response time for end user is improved**. Further advantages are:

- Extremely high **HSM stability and availability**
- It is a commercial **product**, with a clearly defined roadmap
- Administration is easy - all necessary **tools** are available from Worldline
- New requirements are available via software modifications, as opposed to non-updatable SAMs. In this way, **your investment is protected**
- No problems with **2048 bit keys**.
- **Adaptable** for any interface
- **High competence** at Worldline due to deployment of HSMs in other areas, such as banking applications, securing electronic payments, securing prepaid accounts in telecommunication companies and securing applications in the health sector.



Flexible Adaption of the Worldline HSM Solution

Future-proof

Check-In / Check-Out Data Volume
Transport associations are actively involved in Check In / Check Out pilot schemes: this will dramatically increase the incoming data volumes at the collection devices. These volumes' transport security presents no problems for the HSMs.

Use of NFC Smartphones
Smartphones could replace chip-cards in the future, i.e. the personalisation tasks have to be facilitated in the smartphone. These new devices, with their virtualised chip-cards, will also be supported by the SAM-Server.

Ticketing System Interoperability
In the current market, there are the first trends at creating interoperability between the most dominant European ticketing systems (OSPT). Any cryptographic changes can be readily implemented on the HSM.

Multi-Modality
In the future, journeys will be increasingly undertaken through the use of various travel methods and the eTicket will become a mobility card. The security requirements involved here can be covered by the HSM.

Certifications

ZKA/DK and VISA certified
FIPS140-2 level 4 certified Hardware
U/L 94V-0 non flammable
ISO 9001:2000
CE approval: EN 55022 class B

References

Payment networks applications
POS network operations
Support of all acquirer protocols
Card issuer authorization and personalisation
Multiple standards of Electronic Purse

Telecommunication
Voucher Management
Electronic direct Top-Up's

Health sector
Generation of card data for health insurance cards
Transport encryption according to standards defined by Gematik
Secure messaging

Energy market / Smart Grid
Personalisation of devices / electricity meters
Authentication and Transport-encryption following DLMS & BSI

Summary

The Worldline HSM offers an efficient, powerful, reliable and future-proof alternative for securing eTicket systems.

For more information:
Please contact: **infoWL-de@worldline.com**

de.worldline.com

The mark of responsible forestry