www.arx.com

# PrivateServer™

## Hardware Security Model (HSM)

Scalable

Reliable

Flexible

Secure

Compliant

# PrivateServer™ HSM

**PrivateServer, ARX's multipurpose, network attached, Hardware Security Module (HSM), provides a secure environment for conducting sensitive cryptographic operations, secure key storage, and management of a large number of keys. PrivateServer offers a cost effective, highly secure (FIPS validated), and reliable solution.**

PrivateServer is a high-performance cryptographic device that offers solutions to a wide range of industries, including financial, commercial, and governmental. PrivateServer can be successfully integrated with the following:

- PKI applications and digital signatures
- Data preparation and personalization for EMV cards
- Payment-cards processing (magnetic and chip cards)
- Bank clearing: VISA authenticated Payment Program-3D Secure, MasterCard Secure Payment Application (SPA), and EMV-CAP applications
- Other applications, such as e-Passport applications, e-Billing, and e-Invoicing.

## PrivateServer Security Capabilities

**A secure communication channel** between applications and PrivateServer that prevents data exposure to malicious users.

**Strong user and application authentication options** that enable an organization to select smartcard or authentication for each user or application accessing PrivateServer.

**Internal secured audit logs** that record information such as errors, cryptographic operations performed, and maintenance events.

**Strict access rights** used to determine the extent in which applications or users are allowed to access certain keys or to perform certain administrative operations.

**Definition of key usage** ensuring the keys meant for certain operations cannot be used for other purposes.

**Secure key uploading mechanisms** that include all methods defined by Visa and MasterCard.

**Secure backup/restore operations** that allow for clone creation of a certain PrivateServer for high-availability and load balancing solutions.

## PrivateServer HSM

PrivateServer is a **FIPS 140-2 Level-3 validated, secure, tamper-evident device**. PrivateServer incorporates a range of security measures to protect the highly sensitive information maintained by an organization. All sensitive operations are conducted within PrivateServer's physically secure casing.

Advanced security features, such as strong user authentication, internal audit mechanisms, and strict access rights to sensitive keys and operations, are all built-in the product.

PrivateServer usage is strictly managed by its secure internally-mounted keys. All security regulations and standards that are defined by VISA and MasterCard are implemented by the PrivateServer HSM.

## Multiple Functionality Device

**EMV Data preparation and personalization:** PrivateServer enables financial institutes to issue EMV payment cards or other types of cards such as cash and loyalty cards. PrivateServer supports the entire issuing process, including cryptographic data preparation of keys and PINs, as well as card personalization.

**Financial transaction authorization:** PrivateServer can authorize EMV or magnetic stripe-based financial transactions. PrivateServer is a good match for EMV-CAP deployment, where the amount of required transaction authorizations per second may rank in the thousands.

**Digital signing engine and PKI functionality:** PrivateServer delivers PKI capabilities including RSA key generation, key import/export operations, key and certificate storage, and digital signatures.

**Secure electronic transaction:** PrivateServer can be used for encrypting, signing, and verifying sensitive information. PrivateServer authenticates the sender, ensures data integrity, and provides non-repudiation.

**PIN Mailer:** PrivateServer HSM can securely output a PIN Mailer to a printer that is attached to the appliance.

## High Volume Key Storage and Management

PrivateServer has the capacity to store and manage a large number of keys in its internally-secured database, thus eliminating the need for the application to manage an external key database. This design also prevents the transfer of keys and other sensitive information across a network.

In-depth key management capabilities offer organizations a sophisticated and innovative method of managing their cryptographic keys. This approach provides for tighter access control of the highly sensitive keys. This assures keys are never accessed and used by non-authorized entities.

## Ease of Network Management

PrivateServer is an easy-to-deploy, easy-to-manage device. PrivateServer includes user friendly graphical management tools that enable administrators to easily and securely perform management operations such as the monitoring of activities within PrivateServer and management of the keys. Using these tools, the administrator can remotely manage users and sessions, and assign authorization rights to keys from their own desk.

Multiple, independent applications running on different application servers can access a single PrivateServer HSM concurrently, eliminating the need to install a separate HSM for each application server. Consequently, PrivateServer offers a solution that is highly cost-effective as it maximizes an organizations ability to conduct transactions.

PrivateServer supports various high-availability configurations and is capable of balancing workloads between multiple HSMs, thereby allowing organizations to conduct a large number of mission-critical and high-volume transactions.

PrivateServer is accessible by the application servers through the network, in contrast to HSMs that are physically attached to the host and require hardware modifications for the installation. Important administrative operations such as backup, viewing the audit log, and monitoring HSM activity are performed remotely, independent of the application.

## High Performance

PrivateServer offers superior performance of both symmetric and asymmetric cryptographic operations. PrivateServer achieves over 5000 symmetric transactions per second and up to 500 RSA signatures per second using a 1024 bit RSA key.

## The Confidence of Authorization and Control

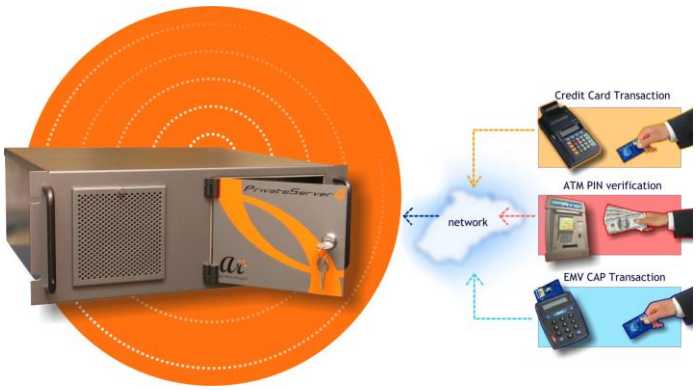
PrivateServer provides strict user access control to all keys and operations. Only authorized users with the appropriate permission have access to PrivateServer operations and to specific keys. Users can only perform the operations that a supervisor has granted them the privilege to perform. Keys may be classified according to type and usage. Setting access rights to particular keys provides the organization with enhanced key protection and controls the users' ability to conduct certain operations .

## The Strength of Compatibility

PrivateServer integrates easily with common industry applications using standard APIs such as PKCS#11, Microsoft CAPI and JCA, thus offering convenient standard interfaces.

## Flexible, Customizable and Reliable Experience

Standard PrivateServer software modules are available for upgrading and meeting various customer requirements without the need to change physical hardware. Additionally, ARX provides customers with the ability to develop and upload customized software modules for self-installation on PrivateServer.




PrivateServer™

# Technical Specifications

PrivateServer™
Hardware Security Module (HSM)

PrivateServer

**Asymmetric Encryption Algorithm**
- RSA (320-4096 bits)

**Symmetric Encryption Algorithms**
- DES
- Triple-DES
- AES

**Security and Standards Certifications**
- FIPS 140-2 Level 3
- FCC Subpart B Class B
- EN 55022 Class B for AC mains and Ethernet lines
- EN 55024
- UL and CB Certified

**Connectivity**
- TCP/IP Ethernet

**PKI Vendor Compatibility**
- Microsoft CA (Win 2000, 2003 server)

**Authentication Modes**
- Smartcard (Windows only)
- Software Key (Windows, Linux, HP, AIX and Solaris)

**Performance**
- 500 RSA Signatures per second (1024 bit keys)
- 5000 triple-DES based operation per second

**Hash Functions**
- SHA-1, SHA-256, SHA-512
- MD5
- ISO-Hashing
- ARDFP

**Secure Key Storage**
- Yes (various configurations support over 100,000 keys)

**Remote Management**
- Yes

**Cryptographic API Support**
- PKCS#11
- Microsoft-Cryptographic API (CAPI)
- Java (JCA or extended)

**Operating System Support (Client)**
- MS-Windows 2000, XP, 2003
- Sun/Solaris (32 or 64 bit)
- HP-UX
- IBM AIX (32 or 64 bit)
- OS/2
- Linux
- STRATUS/VOS
- Tandem
- MVS/OS390
- OpenVMS

**Physical Dimensions**
- W x L x H: 48.3x44.7x17.8 cm
- 4U Rack Mountable
- Weight: 15Kg

www.arx.com
US Headquarters: 855 Folsom St. Suite 939, San Francisco, CA 94107 Tel: (415) 839-8161 Fax: (415) 723-7110
International Headquarters: 10 Nevatim St, Petach Tikva, Israel. Tel: +972-3-9279500 Fax: +972-3-9230864