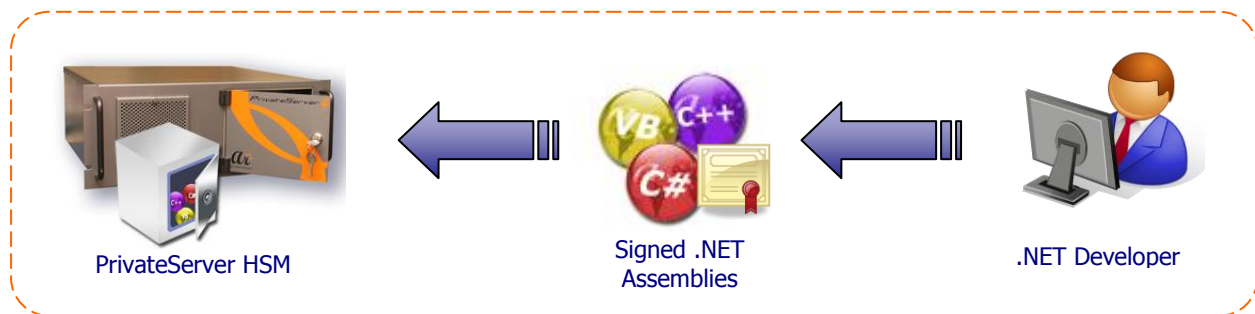


# PrivateServer Module Development Kit

## General Information

PrivateServer™ is a highly secure (FIPS 140-2 Level 3 validated), network attached, Hardware Security Module (HSM) that provides an environment for conducting sensitive cryptographic operations, secure storage and management of a large number of keys.

A major feature of PrivateServer is its Module Development Kit (MDK). The MDK enables customers and partners to develop their own custom modules that will be executed inside the HSM in order to secure their cryptographic mechanisms. The new MDK also allows application code to be securely executed within the PrivateServer HSM environment.



## PrivateServer MDK Features

### Custom Module Development

- ▶▶ PrivateServer MDK takes full advantage of the .NET environment and development tools to allow third parties to develop code that access the functionality of the PrivateServer API and performs cryptographic operations, generates keys and runs numerous other applications. The code is based on programming languages and tools supported by .NET Framework 2.0. These include: C#, VB .NET, Microsoft Visual Studio 2005 and many others.
- ▶▶ The interfaces to the module are based on XML input and output structures.
- ▶▶ Multiple modules may be loaded into the PrivateServer, each running in a separate application domain. These application domains run in a restricted sandbox to protect the security and stability of the PrivateServer HSM.
- ▶▶ ARX supplies an environment that enables the developer to debug the module externally before uploading it to the PrivateServer HSM. The entire debugging procedure is based on Microsoft Visual Studio 2005.
- ▶▶ After the module is debugged, it can be loaded to the HSM without any modification. The same client application that was used to test and debug the module externally can be used to test it inside the PrivateServer HSM.
- ▶▶ ARX provides code samples illustrating the correct usage of the MDK.
- ▶▶ ARX provides an additional by-product of the MDK, which is a .NET wrapper to all the existing PrivateServer API functions. This wrapper is implemented as a .NET Assembly, and can be used to develop .NET applications that use cryptographic operations of the PrivateServer, such as Web Server applications.

## Uploading the Modules to the PrivateServer HSM

---

- ▶ Once compiled into a .NET Assembly, the module may be securely uploaded to the PrivateServer HSM. The partner/customer will be provided with a special developer signature key and a certificate by ARX that will be used for signing the module, thus making sure that only authorized and approved modules may be uploaded to the HSM.
- ▶ The loaded modules are encrypted and signed, protecting the code from being reviewed or altered by unauthorized persons. This enables organizations to securely distribute the modules to other customers.
- ▶ There are restrictions applied by the PrivateServer HSM for upload and executing the modules in order to avoid exploiting of the PrivateServer HSM by a downloaded module or compromising its security or stability.
- ▶ The new functions may be invoked from any platform such as Windows, Unix, Linux, IBM Mainframe, or others. The modules may be accessed using any programming language such as C/C++, Java, C#, VB .NET etc.
- ▶ The modules operate in the context of the authenticated user, so they cannot perform operations that are not allowed for the specific user.

## Limitations, Restrictions and Licensing

---

- ▶ The MDK functionality is based on PrivateServer version 4.5 and is not supported with earlier versions of PrivateServer HSM.
- ▶ An MDK license is required for any PrivateServer HSM that runs a downloadable module.