

## Intel Releases BIS Server Components as Open Source

Chet Johnson  
Strategic Marketing Manager  
Intel Architecture Lab  
Intel Corporation

## Table of Contents

(Click on page number to jump to sections)

<b>INTEL RELEASES BIS SERVER COMPONENTS AS OPEN SOURCE.....</b>	<b>3</b>
OVERVIEW .....	3
SECURITY FOR REMOTE MANAGEMENT .....	3
BUSINESS BENEFITS FOR DEVELOPERS .....	4
OPEN SOURCE MANAGEABILITY TECHNOLOGY FOR THE EFI .....	4
SUMMARY .....	4
MORE INFO.....	5
AUTHOR BIO .....	5

DISCLAIMER: THE MATERIALS ARE PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OF INTELLECTUAL PROPERTY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE MATERIALS, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME JURISDICTIONS PROHIBIT THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. INTEL FURTHER DOES NOT WARRANT THE ACCURACY OR COMPLETENESS OF THE INFORMATION, TEXT, GRAPHICS, LINKS OR OTHER ITEMS CONTAINED WITHIN THESE MATERIALS. INTEL MAY MAKE CHANGES TO THESE MATERIALS, OR TO THE PRODUCTS DESCRIBED THEREIN, AT ANY TIME WITHOUT NOTICE. INTEL MAKES NO COMMITMENT TO UPDATE THE MATERIALS.

Note: Intel does not control the content on other company's Web sites or endorse other companies supplying products or services. Any links that take you off of Intel's Web site are provided for your convenience.

## Intel Releases BIS Server Components as Open Source

Chet Johnson  
Strategic Marketing Manager  
Intel Architecture Lab  
Intel Corporation

---

### Overview

The ability to boot a PC to a known software configuration over the network has become widespread since the introduction of products that implement the Preboot Execution Environment (PXE). In some business environments, concerns over the security of preboot operations have delayed PXE usage, but now a standards-based solution known as Boot Integrity Services (BIS) is available. BIS plays an important role in helping safeguard PC integrity before a PC is fully operational.

As with PXE, BIS includes both a client component implemented in the system BIOS and a server component implemented in a management application. To encourage widespread support of BIS in application software, Intel is releasing the code for the BIS server component as open source. Software developers that have implemented support for PXE technology can use BIS to improve the security of a PXE network boot. BIS server components complement the BIS API (application programming interface) and services that are now becoming available on Wired for Management (WfM) enabled PCs.

The BIS server component is based on Common Data Security Architecture (CDSA) software that is also available as royalty-free open source. Unlike proprietary techniques to improve pre-boot security, BIS usage of CDSA builds upon widely accepted security-related standards including RSA or DSS digital signatures, X.509 v3 digital certificates, and Signed Manifest data integrity credentials.

Several business models of desktop PCs from IBM, Dell, and Compaq are now available with BIS as a complement to their PXE implementations. On the server side, BIS support has already been incorporated into systems management applications from Altiris, Inc., Computer Associates International, and ON Technology. Both PXE and BIS are identified in the PC 2001 System Design Guide for platforms supporting Microsoft\* Whistler operating system.

### Security for Remote Management

Installing new software on a PC over the network can make the PC vulnerable to unauthorized use, tampering, and accidental misconfiguration. Once exposed to such a threat, a PC's state is suspect. To help remedy this situation, a BIS API that employs public-key cryptography was defined. The BIS API enables preboot management applications to check the integrity and authorization of programs and data that are downloaded over the network. This check provides a more secure and interoperable remote boot security solution for managed PCs.

The PXE remote boot facility is the principal user of BIS to help keep client PCs safe from unauthorized access, although other software designed to run preboot may make use of these services. Initial setup of BIS and its operational usage can be characterized by the following steps:

1. *Key-pair generation.* BIS server components generate a public and private pair of cryptographic keys in the server environment. These keys identify the administrator of the client PCs that will receive downloaded programs and data and are owned by the administrator.
2. *Client configuration.* The administrator's public key is embedded into a digital certificate that is stored on each client PC.
3. *Data signing.* The administrator's private key is used to create a digital signature on the management server for each program or data file to be downloaded to a client during preboot management.
4. *Verification on download.* Whenever the management application downloads a program or data to the client during a preboot management operation, the corresponding digital signature file is also downloaded. The client program that performs the download then calls the BIS API to perform verification before allowing the data to be used or the program to be executed. BIS checks that the digital signature corresponds to the combination of the downloaded program or data as well as to the key pair for which it has the public key.

### ***Business Benefits for Developers***

The design of BIS server components is based on the CDSA (Common Data Security Architecture) specification. CDSA gives application developers access to security services by implementing a “middleware” layer between applications and security services. Instead of writing an application for a specific security service, developers write to a standard application programming interface (API). Stable, well documented APIs allow rapid adoption of emerging technologies, decrease application development cost, and reduce time-to-market by letting developers stay focused on enhancing their applications rather than building discrete security solutions.

In addition to enabling worldwide use of CDSA, BIS, and PXE technology, open source software has the advantage of lower costs, greater industry attention, and increased collaboration. CDSA, BIS, and PXE source code are publicly available for download on the Internet, free of charge from the Intel Developer Web site. Companies can view the source code to verify for themselves that no “backdoors” or security holes exist in the software.

Open source allows reuse of protocol components to ensure interoperability. Experience with open source technology such as the Linux\* operating system reveals that companies can often resolve problems by examining and modifying the working code, or by collaborating with open source developers on a fix. Ultimately, the result of this open scrutiny and collaboration is software that is significantly more robust and reliable.

As a result of a recent and groundbreaking change in U.S. encryption regulations, open source security software such as CDSA and BIS can now be freely exported (except to Cuba, Iraq, Libya, Yugoslavia, North Korea, Iran, Syria, and any other country against which the U.S. has a goods embargo). This fundamental change in regulations ends the isolation between developers in different countries and allows standards-based security code to be available for use worldwide.

### ***Open Source Manageability Technology for the EFI***

To help solve certain technical BIOS boot issues, Intel has worked with several other vendors in the definition of an Extensible Firmware Interface (EFI). EFI is an OS- and platform-independent boot and preboot interface that is being implemented in new Intel® Architecture platforms including those implementing the Intel® Itanium™ processor. The EFI specification includes PXE as an existing open industry specification for enterprise network clients to automatically download software images and configuration parameters.

The EFI specification defines a new model for the interface between operating systems and platform firmware. The interface consists of data tables that contain platform-related information, plus boot and run-time service calls that are available to the operating system and its loader. Together, these provide a standard environment for booting an operating system and running preboot applications.

### ***Summary***

Intel is releasing as open source the code for the BIS server components. Initially, this software is for use on servers implementing Microsoft Windows NT\* or Windows 2000 server. Before the end of the year, variations for servers running the Linux operating system and for platforms implementing EFI will be available for download. BIS server components can be deployed royalty free to enhance the security of PXE-based preboot operations without using proprietary techniques.

BIS is based on CDSA, which is being widely adapted by hardware and software vendors and is also available as open source. The release of PXE and BIS open source to the software developer community is intended to encourage developers to create more applications for the server side of PXE, and to include BIS when they do so.

### **More Info**

For more information on BIS API, read [Safeguarding the Integrity of Managed PCs](#).

For more information regarding CDSA, read [CDSA Brings Security into the Open](#).

### **Author Bio**

Chet Johnson joined Intel in 1997 and led efforts with major systems management software vendors to support the Wired for Management (WfM) initiative and WfM-enabled platforms. He currently works in Intel's Architecture Lab, with marketing responsibilities centered on networking technologies. Chet received a B.S. in electrical engineering from the University of Minnesota's Institute of Technology.

*—End of Intel Developer Update Magazine Article—*