



*Find out what you need to start using the BlackBerry Smart Card Reader for controlled access to BlackBerry smartphones and computers.*

## Technical Requirements: BlackBerry Smart Card Reader

*Making It Easier Than Ever to Comply with Operational Requirements for Multi-factor Authentication*



## Technical Requirements for the BlackBerry Smart Card Reader

The BlackBerry Smart Card Reader builds on the security, flexibility and mobility of the trusted BlackBerry Enterprise Solution.

The BlackBerry® Smart Card Reader allows mobile personnel to meet operational requirements for using multi-factor authentication with Bluetooth®-enabled Microsoft® Windows® computers, BlackBerry® smartphones, PKI applications and for secure web browsing.

The BlackBerry Smart Card Reader is designed to help prevent unauthorized access to computers and BlackBerry smartphones. Instead of using a stationary reader or bulky peripheral that can be left behind easily, users insert smart cards into lightweight, portable BlackBerry Smart Card Readers that they carry with them at all times. BlackBerry smartphones and computers that are paired with a BlackBerry Smart Card Reader lock when the user and the BlackBerry Smart Card Reader go out of range.

The BlackBerry Smart Card Reader enhances the authentication model for access control by introducing an additional proximity-based factor through an AES-encrypted Bluetooth connection.

The BlackBerry Smart Card Reader can replace serial or USB based PC smart card readers, even if your organization has not deployed a BlackBerry solution.

REQUIRED COMPONENTS	
Smart Card	The BlackBerry Smart Card Reader is designed to support all ISO-7816 smart cards.
Smart Card Drivers	Software drivers must be installed for the BlackBerry Smart Card Reader to communicate with smart cards. Drivers are available for Personal Identity Verification (PIV) cards, Common Access Cards (CAC) and Safenet 330 cards. Vendors and customers can also write their own smart card drivers for the BlackBerry Smart Card Reader using public APIs in the BlackBerry Java Development Environment.
Public Key Infrastructure	Access to a Public Key Infrastructure (PKI) is necessary to generate the user certificates that are placed on the smart card using the BlackBerry Smart Card Reader and the software provided by the smart card vendor. The PKI can be insourced or outsourced depending on the needs of your organization.
OPTIONAL COMPONENTS	
BlackBerry smartphone	The BlackBerry Smart Card Reader works with all Bluetooth enabled BlackBerry smartphones with BlackBerry Device Software Version 4.0 or later installed.
PC	The BlackBerry Smart Card Reader is designed to work with Bluetooth-enabled Microsoft Windows XP and Microsoft Windows Vista computers. PCs without built-in Bluetooth hardware can communicate with the BlackBerry Smart Card Reader using an external Bluetooth hardware token.
LDAP Directory Service	Using two-factor authentication for computer logon requires an LDAP directory service to confirm the user's identity based on the certificate stored on the user's smart card.
Secure Web Server	Secure web browsing of internal sites requires a web server that supports Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to authenticate the user and create a secure connection.
S/MIME Support Package for BlackBerry smartphones	Signing, encrypting, verifying and decrypting S/MIME email requires the S/MIME Support Package for BlackBerry smartphones.†

### For More Information

To learn more about BlackBerry Smart Card Reader visit:  
[www.blackberry.com/go/smartcardreader](http://www.blackberry.com/go/smartcardreader)

or contact your BlackBerry sales representative

† Available for BlackBerry Enterprise Server for Microsoft® Exchange and BlackBerry Enterprise Server for IBM® Lotus® Domino® only.