

# TRUSTBEARER DESKTOP

## ABOUT

TrustBearer Desktop is a smart card middleware product approved by GSA for FIPS 201 use with PIV cards. It supports authentication, data protection, and digital signing using government-issued smart cards with a variety of desktop and online applications. TrustBearer Desktop works with PIV, CAC and TWIC smart cards.

Unlike traditional client middleware, TrustBearer Desktop provides strong authentication to Web 2.0 applications using a government-issued credential. TrustBearer's identity provider combines the strength of hardware-based PKI authentication with the simplicity and ease-of-use that Web 2.0 users expect.

Download a free, fully functional trial of TrustBearer Desktop:

[www.trustbearer.com/desktop](http://www.trustbearer.com/desktop)

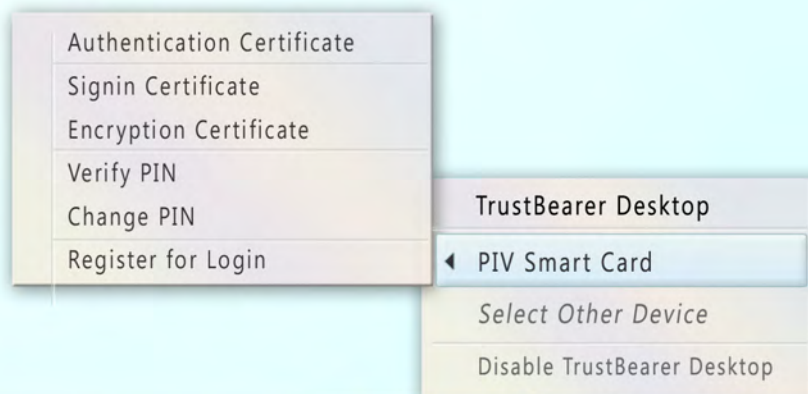
Supported on Windows XP and Vista with browser support for Internet Explorer 6 or above and Mozilla Firefox 2.0 or above

Support for Mac OS X coming soon



## FEATURES

- Secure, smart card login to Windows domains.
- Digital signing and encryption support for Microsoft Outlook using smart card PKI certificates
- Secure smart card login to websites requiring SSL client authentication, with support for Internet Explorer and Firefox.
- VPN authentication
- Digital signing of documents using applications such as Microsoft Word or Adobe Reader
- User PIN management available using the Windows system tray icon



## Desktop Runtime

The architecture diagram below shows the components included in and affected by the TrustBearer Desktop runtime. The runtime provides dynamic support for hardware security devices such as smart cards, hardware & software tokens, trusted platform modules (TPM), and biometric readers. These support modules can be cached locally or network delivered by the TrustBearer Live Server. A single module is compatible with all supported hardware architectures, operating systems, and web browsers.

The TrustBearer Desktop runtime also provides the ability to customize user interfaces (UI) and enforce policies such as PIN length. If a network connection is available, UI and policies can be remotely updated without requiring any user interaction. The runtime engine verifies the digital signature of all modules before they are executed on the client to ensure that they were provided by a trusted source.

## Embedded Solutions

TrustBearer has years of experience developing smart card applications for multi-function printers and scanners, mobile/portable devices, thick client and single-purpose computers, and various network appliances. Our embedded middleware supports CAC, PIV, and TWIC for with a variety of embedded architectures, including Windows Mobile, Linux, and vxWorks.

Learn more at,

[www.trustbearer.com/embedded](http://www.trustbearer.com/embedded)

## Runtime Architecture

