



## Microsoft

Microsoft has deployed a smart card employee identity system that manages both physical access and remote logical access to company networks. Microsoft completed worldwide deployment of the smart ID card at the end of 2002.

With industry-wide security threats to corporate network access increasing, Microsoft initiated the smart card project in late 2000 to implement a two-factor security solution for remote access to company networks. Due to Microsoft's size (more than 61,000 employees in over 400 locations worldwide), managing the security risks inherent in remote access was a critical problem.

Microsoft evaluated a number of technologies before deciding on smart cards, including biometrics, other hardware tokens (e.g., devices that automatically calculate new passwords at specified times and match passwords generated by a similar password-changing device on an authentication server), and USB token-reader devices similar to smart cards. Microsoft chose to deploy smart card technology due to the combination of reliability, performance, cost, features, mobility benefits, and integration with the Windows network environment.

Microsoft has reported the following benefits of deploying employee smart cards:

- Strengthened security. Two-factor authentication with smart cards (requiring both the smart card and PIN) provides stronger security than simply entering valid credentials.
- Increased flexibility. Smart cards carry security certificates and can be used for other projects. The ability of smart cards to support other applications (such as digital e-mail signatures, document signatures, personal data storage, and personal payment systems) was viewed as a key benefit.
- Ease of use. Users find smart cards simple to use, with no bulky device to break or cumbersome password generator to carry. Microsoft designed the smart card implementation to minimize the impact on users when using the smart card during the remote authentication experience. The smart ID card was also a familiar form factor, since employees already carried an RFID-style photo ID cardkey to access buildings. By implementing a smart ID card that combined the smart chip and RFID capability, Microsoft avoided requiring employees to carry (and possibly lose) an additional card.
- Leverage of existing infrastructure. Microsoft uses the PKI capabilities native to Windows 2000 Server and Windows 2003 Server to create security certificates and manages the process internally.

---

*This profile extracts content from the Microsoft white paper, "Smart Card Deployment at Microsoft," March 11, 2004, available at <http://www.microsoft.com/technet/itsolutions/msit/security/smartcrd.mspx>.*

*The profile was published in the Smart Card Alliance report, "Logical Access Security: The Role of Smart Cards in Strong Authentication," available at [http://www.smartcardalliance.org/alliance\\_activities/logical\\_access\\_report.cfm](http://www.smartcardalliance.org/alliance_activities/logical_access_report.cfm). For more information about how smart cards are used for secure identification applications, visit the Alliance web site at <http://www.smartcardalliance.org>.*