

# Security product comparison matrix



Technology	Privaris plusID™ Token	Prox Cards	Smart Card Technology	Fingerprint Readers Installed at Doorways	PC-Integrated or USB-Connected Fingerprint Readers
<b>Built-in fingerprint reader in a convenient, wireless token</b> <ul style="list-style-type: none"> <li>eliminates need for fingerprint readers at every door and PC</li> <li>upgrades security at every access point</li> <li>eliminates personnel back-ups caused by door mounted sensors</li> <li>no single point of failure, reduced maintenance</li> <li>eliminates personal hygiene and health issues</li> </ul>	<b>YES</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>
<b>Add biometrics without changes to existing physical and logical security infrastructure</b> <ul style="list-style-type: none"> <li>works with MS Windows Server exactly like a smart card for logon, over USB</li> <li>interfaces with standard proximity, iCLASS and similar door readers</li> <li>supports one-time password implementations for local and remote access to IT systems</li> <li>low cost, rapid implementation; no middleware, wiring or coding required</li> <li>permits a partial biometric deployment for select employees or areas</li> </ul>	<b>YES</b>	<b>NO</b>	<b>NO</b> , requires installation of fingerprint readers for doorways and PCs	<b>NO</b> , requires installation of fingerprint readers at doorways	<b>n/a</b>
<b>On-device fingerprint enrollment and matching</b> <ul style="list-style-type: none"> <li>allows for more accurate fingerprint matching algorithms</li> <li>faster match times (a second or less)</li> <li>users control the storage and processing location of their biometrics</li> <li>fingerprint template securely stored and can not be compromise</li> <li>device is reclaimable and reusable</li> </ul>	<b>YES</b>	<b>NO</b>	Not possible on smart card alone, requires the addition of an external fingerprint reader	Fingerprint transmitted to centralized database for matching, or done locally in door reader	PC-Integrated = yes USB-Connected = no
<b>No biometric database required</b> <ul style="list-style-type: none"> <li>eliminates the security risk of moving the fingerprint to a database or door reader</li> <li>no hacker target</li> <li>no risk or expense of protecting a database of fingerprints</li> <li>no additional hardware, software or connectivity required</li> <li>users' never have to share their sensitive biometric data with a third party</li> </ul>	<b>YES</b>	<b>NO</b>	For match-on card technology only, but requires fingerprint transfer from external system to the card	<b>NO</b>	A database may or may not be used but fingerprint data is stored locally on the PC
<b>Cryptographic services provider</b> <ul style="list-style-type: none"> <li>encrypted communication</li> <li>digital signatures</li> <li>time based algorithms</li> <li>random data generation</li> <li>provides for standard interfaces to logical applications</li> </ul>	<b>YES</b>	<b>NO</b>	<b>YES</b>	<b>NO</b>	PC-Integrated = yes USB-Connected = no

# Security product comparison matrix

Technology	Privaris plusID™ Token	Prox Cards	Smart Card Technology	Fingerprint Readers Installed at Doorways	PC-Integrated or USB-Connected Fingerprint Readers
<b>Convergence of physical and logical (IT) security in one device</b> <ul style="list-style-type: none"> <li>one device replaces multiple access cards, fobs and passwords</li> <li>greater and faster return on investment (ROI) through convergence</li> <li>access to multiple facilities (supports multiple card formats)</li> <li>secure logon to PC's, applications, websites and encrypted files</li> <li>provides a non-repudiable audit trail for regulatory compliance</li> </ul>	<b>YES</b>	<b>NO</b>	Requires a PC-connected reader for logical access. Only reusable if smart card does not include a photo	<b>NO</b>	<b>NO</b>
<b>Supports 3-factor authentication</b> <ul style="list-style-type: none"> <li>dramatically heightens security levels</li> </ul>	<b>YES</b>	<b>NO</b>	<b>NO</b>	Only if a PIN pad is included on reader	<b>NO</b>
<b>Highest levels of security and speed</b> <ul style="list-style-type: none"> <li>all sensitive biometric data encrypted and securely stored on device</li> <li>employs a 150 MHz secure RISC processor (BCM 5890)</li> <li>tamper resistant (designed to meet FIPS 140-2 Level 3 US Govt. standard)</li> </ul>	<b>YES</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>	<b>NO</b>