Gemalto Strong Authentication Devices

FINANCIAL SERVICES & RETAIL

ENTERPRISE>PRODUCT

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATIONS

gemalto
security to be free

Gemalto Strong Authentication Devices

> Static Passwords Are Not Enough

Enterprises face numerous challenges in protecting their networks, highly sensitive data, and employees' identity information. As they invest in security solutions for these needs, several requirements and use cases must be considered. For example, employees need to connect to enterprise networks not just from the office but from anywhere, whether from home, an airport kiosk or a customer location. Access is required from desktops, laptops and mobile devices, and data is becoming highly portable, making it more susceptible to loss or unauthorized access. And using a single identity credential to protect digital information – and to secure access to offices and facilities – opens up a range of opportunities to strengthen security and enhance usability for employees.

Gemalto uniquely meets these needs with smart card-based solutions that provide strong authentication using one-time passwords (OTP) and the ability to implement Public Key Infrastructure (PKI) and physical security systems.

Empowered by the Gemalto Strong Authentication Server (SAS), a family of smart card devices offers several form factors to handle the range of use cases involved in securing network access, sensitive data, and digital identities throughout the enterprise. Both unconnected and connected (via USB) modes of operation are supported and the same end-user devices can be deployed for strong authentication with OTP and for PKI applications. In addition, some USB devices provide up to 2 GB of secure data storage to protect mobile data inside and outside the office.

Gemalto .NET end-user devices are also interoperable with Windows® operating systems, Microsoft® ILM 2007 and other components in Microsoft's security platform. The Gemalto .NET smart card is natively supported in Windows Vista® and Server 2008 and supported via Windows Update for Windows XP & Server 2003. This makes it easy to deploy and manage strong authentication and PKI systems without additional software or middleware. They can be deployed in Microsoft environments for:

- Strong Authentication using OATH compliant OTP or X509 digital certificates
- Windows Logon
- Secure remote, VPN and Web Access
- Document, file and email encryption
- Digital Signatures for Outlook email and Microsoft Word and Excel documents

	Easy OTP	.NET Key	.NET Dual	.NET Card	SEG
	Secure remote access using OTP authentication Unconnected operation for secure access from anywhere	Ideal solution for multi - application use of OTP and PKI Connected operation for automatic entry of OTP	One device for OTP strong authentication and PKI services Maximum flexibility for connected and unconnected operation OTP via display or auto entry via USB	Card form factor for deploying PKI services Supports OTP for remote access Can be deployed as a corporate badge for physical and logical access	Personal Portable Security Device Supports OTP and PKI Up to 2GB of secure flash storage and portable applications
OTP Display	•		•	•	•
Customizable Display	•		•		
Automatic OTP Entry		•	•	•	•
PKI (Digital Signing or Encryption)		•	•	•	•
Physical Access (Office Building)				•	
Secure Storage					•
Windows PKI Compatibility (no middleware)		•	•	•	•
USB Port Control					•
PKCS11 Support		•	•	•	•

© 2008 Gemalto. All rights reserved Gemalto and the Gemalto logo are trademarks and service marks of Gemalto NV and are registered in certain countries. April 2008 CC

www.gemalto.com/enterprise

gemalto
security to be free