FOR IMMEDIATE RELEASE

Contact: Dovell Bonnett
Founder and CEO
Access Smart, LLC
Tel: (949) 218-8754
e-mail: dovell@access-smart.com

Power LogOn® Authenticates User into Microsoft's Forefront

Microsoft®'s Forefront Needs More Than Identity Management for Cyber Attack Prevention

Ladera Ranch, CA – October 01, 2011 – Access Smart® Announces the Interoperability of their Power LogOn® Password Manager with **Microsoft® Forefront**. Microsoft 's Forefront Identity Manager (FIM) 2010 provides IT with the tools needed for identity and access management through a SharePoint-based policy management console. Microsoft correctly targets the importance of identity management for users, devices, and services due to cyber attacks, regulatory mandates and privacy protection compliance. While FIM 2010 is designed around secure identity management, the logical question follows: How is the user properly identified during Windows authentication?

FIM 2010 has integrated passwords and certificates functions with smartcards to deliver a secure network. If the first link in the chain is insecure then the entire network is also insecure. Can you really trust and know who really is logging in, accessing files or purchasing unauthorized services? Smartcards two- or three- factors of authentication capabilities are a key component to establish trust.

Users who manual type in a user name and password are the weakest link in computer, network or cloud authentication. Not because passwords are insecure, but because how users choose and manage their passwords.

- Using a simple, easy to remember password
- Password written on sticky notes and posted on their monitors
- Using the same password for the company's network as they use for their PlayStation account
- And not having proper malware protection on a home computer that allows thieves to steal passwords with a keylogger.

When combined with the functions and features of an ID badge, smartcards gives IT a single, secure credential to control the issuance, management and access within an entire organization. From the user's perspective they insert a card into a reader, type a single PIN and/or present their finger to a biometric reader and that's it. FIM 2010 does the rest. A win-win for IT since they have increased security and it's convenient for the user – no more complex passwords to remember or type.

But which smartcard authentication is best, a password manager or a digital certificate. Both technologies have their pros and cons (see our "Security Technology Comparison" white paper). The better questions are: what is the environment, cost considerations, time to implement, value of data being protected, etc.? Certificate systems, especially Public Key Infrastructure (PKI), are very secure but also very expensive for most businesses to implement. Many systems require expensive smartcard chips, hardware modifications to the server, relationships with Certificate Authorities, annual certificate renewal fees, non-transferal of certificates when there is employee turnover, advanced IT training, and typically years to fully integrate. Certificates are great for those people that have to digitally sign documents and want the non-repudiation, but it's not something every employee needs.

Access Smart created a secure password manager for Windows called Power LogOn. The user simply authenticates themselves with a PIN and/or biometric.

- No more manually entering passwords that keyloggers can pick up.
- No more employees writing passwords on sticky notes for others to find.
- No more using the same simple password for every account.

Since Power LogOn has no annual subscription/renewal fees, no back-end server modifications, no extensive training and licenses are transferable makes Power LogOn affordable from the single business owner up to the large corporations, agencies and institutions. Power LogOn usually takes IT only a couple of days to fully implement thus implementing security faster than any certificate based solution. Power LogOn can also be configured to deliver up to 8-levels of authentication assurances.

- Something you have
- Something you know
- Something you are
- Something the card has
- Something the card knows
- Something the server and card knows
- Something an application and card knows

FIM 2010 focuses on Identity Management and Power LogOn addresses user authentication; together businesses and their employees have an integrated permissions based secure network. IT can eliminate the manual logon processes that cannot truly authenticate a user. Finally, with the low cost of ownership security is no longer determined by accountants but by the businesses desire to deliver privacy protection confidence to their customers.

About Access Smart

Founded in 2005 and headquartered in Ladera Ranch, California, Access Smart delivers Access-as-a-Service (AaaS) solutions by way of a password manager for Windows authentication to reduce the risk of cyber-attacks. Access Smart implements AaaS using contact or contactless smartcards, magnetic stripe or 125kHz Prox technologies. The value that Access Smart brings is to offer more security functions and affordability onto a single employee ID badge. Please contact Access Smart as to discuss how best to implement Authentication, Authorization and Non-Repudiation into your business. Access Smart – The Easy, Affordable Alternative to PKI. For more information about Access Smart, please visit http://www.Access-Smart.com.

Access Smart and Power LogOn are registered trademarks exclusively licensed to Access Smart, LLC. Other product names are either trademarks or trade names of their respective holders.