authentication, where the user only has to enter the PIN when logging in to the computer. From there on Hash Guard regularly checks incoming connections to the servers. For each authentication request to a server Hash Guard will assure the legitimacy of the connection by verifying the presence of the user’s smartcard at the requesting computer.

Hash Guard protects protocols that employ the LAN Manager (LM) or NT LAN Manager (NTLM) as well as Kerberos authentication including Server Message Block (SMB), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) and more. Modifying these protocols is not necessary.

Partner
Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space, run the Stormshield brand and offer innovative end-to-end security solutions worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security). Arkoon Netasq implements Hash Guard in Stormshield products.

Benefits
- Effective protection against one of the most dangerous and common sort of targeted attacks on Windows domain networks
- Easy to integrate into enterprise networks
- Ease of use/single sign-on
- Standard conform smartcard protocols (ISO/IEC 7816)