Executive Brief

Wave Virtual Smart Card for HSPD-12:
Two-Factor Authentication for Logical Access

Wave Virtual Smart Card 2.0 provides strong two-factor authentication, offering better security at less than half the cost. It can be used like a traditional smart card or USB security token – but because it uses hardware already embedded in the endpoint, the user doesn't have to carry anything extra for secure authentication. Typical use cases are for secure VPN, web applications and other certificate-based applications, like 802.1x, remote desktop, or user login to a Windows tablet or laptop.

Wave Virtual Smart Card 2.0 Value Proposition:

Better Security: Uses the industry-standard hardware Trusted Platform Module (TPM), so built to vendor-neutral, internationally-developed security standards. The keys are unique to each endpoint, i.e. it is not vulnerable to a centralized server hack.

Instantly mitigates the threat from compromised user credentials: By applying a strong, hardware-based second factor to the authentication process, it negates the huge risk posed by the compromise of user credentials and the potential to use those credentials for unauthorized entry into sensitive IT systems and applications.

Convenient: Built into the endpoint, so there's nothing extra to carry or lose.

Cost-effective: Typically greater than 50% lower total cost of ownership than USB token solutions, in some cases up to 75% less. Leverages pre-existing hardware for lower capital expenditure and eliminates replacement costs for lost tokens and smart cards.

Works right now: The only enterprise-capable virtual smart card that works on Windows 7. Available today on Windows 7, Windows 8 and Windows 8.1.

For use in agencies complying with HSPD-12: FIPS 201 (Personal Identification Card - PIV) is the specification that defines identification requirements that meet HSPD-12. Section 6 of FIPS 201 defines requirements for physical and logical access options using PIV cards. For logical access (FIPS 201 Section 6.3.2), Table 6-3 defines local workstation environment access and remote/network system environment access for OMB E-Assurance Levels 1 through 4 (which correlate to FIPS 201 levels of Little or No Confidence (level 1), Some Confidence (level 2), High Confidence (level 3), and Very High Confidence (level 4)). Although Wave solutions do not apply to the physical access scenario, there are two logical access scenarios that Wave Virtual Smart Card using TPM has a strong use case for. FIPS 201 defines multiple types of authentication options that can be performed with a PIV card; the two authentication mechanisms that map to TPM/virtual smart card are: 1) PKI-CAK and 2) PKI-AUTH.

	PKI-CAK	**PKI-AUTH**
OMB-E Confidence Level	2	4
FIPS 201 Confidence Level	Some Confidence	Very High Confidence
Access type	Local & remote logical	Local & remote logical
Key type	Asymmetric key proves possession of private key (Card Authentication Certificate)	Asymmetric key proves possession of private key (PIV Authentication Certificate)
PIN entry required?	No	Yes – prior to key challenge/ response
Two-factor authentication?	No	Yes

Table: *FIPS 201 Authentication Scenarios Mapping to Virtual Smart Card with TPM*

Wave Virtual Smart Card uses the TPM to provide solutions to frequently encountered authentication problems. Using pre-deployed hardware that is built to an industry security standard allows Wave Virtual Smart Card to introduce strong, two-factor authentication with a low total cost of ownership and ease of use not practical with traditional two-factor products like smart cards and USB tokens.

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

03-000401/ version 1.02 Release Date: 12/02/2014