



# Using Security Middleware to Extend Your PKI Infrastructure

V-ONE SmartGate® application layer security as a PKI enabling technology

---

## White Paper



## Abstract

This paper identifies the key challenges organizations face in implementing PKI solutions and explains how the V-ONE SmartGate® product line can serve as an effective PKI enabler.

SmartGate is a standards-based middleware solution designed to leverage and extend existing PKI functionality. SmartGate includes generic PKI support that allows it to use X.509 digital certificates. The SmartGate software provides authentication based on the user's certificate, AES level encryption for secure data channels, access controls and audit logs. These capabilities allow SmartGate to act as a PKI enabling gateway for legacy application servers *without* requiring any modifications to those servers. All connections to internal resources are authenticated, managed by policy, and logged based on end user certificates issued by trusted authorities.

## Background

As the electronic framework for trusted security, Public Key Infrastructure (PKI) is a combination of software, encryption technologies, and services that protects communications and business transactions on networks like the Internet. PKI uses public- and private-key pairs to digitally sign documents. A digital certificate is an electronic document issued by a third party that acts as electronic identification. It contains the user's public key, which is validated by the digital signature.

Participants in a PKI each obtain a digital certificate from a trusted Certificate Authority (CA). The digital certificate then authenticates their identity when initiating a secure transaction. Individual transactions are encrypted by each participant using their own pair of electronic keys, one of which they keep for their own private use, while the other -- the 'public key' -- is made available to other participants. PKI has been adopted as a basis for secure Internet and web services transactions.

The recognized standard X.509 Public Key Infrastructure defines the format of the digital certificates as well as the protocols used for validating and revoking those certificates. These certificates can be stored in a file format or can be written to smart cards. The PKCS<sup>1</sup> #11 standard specifies an API<sup>2</sup>, called Cryptoki, to devices that hold cryptographic information and perform cryptographic functions. The PKCS #12 standard specifies a portable format for storing or transporting a user's private keys, certificates, and miscellaneous secrets, such as a CAC<sup>3</sup>, Smart Card or DataKey.

A PKI provides a solid framework for authentication and encryption. The X.509 standard has a long history and has proven itself viable over time. As government and commercial organizations begin to implement PKI, challenges arise testing the ability to implement, deploy, and manage large numbers of certificates. Issues such as lack of interoperability with legacy applications, and fine-grained access control also need to be addressed.

---

<sup>1</sup> Public Key Cryptography Standards

<sup>2</sup> Application Program Interface

<sup>3</sup> Common Access Card

## **Meeting PKI Implementation Challenges**

### ***Leveraging IT Investment***

The high cost of implementation and the interoperability problems associated with PKI technology are the key reasons why organizations are not moving ahead with or are scaling back their PKI implementation plans.<sup>4</sup>

V-ONE's SmartGate technology can cost-effectively enable your existing applications to interoperate with your PKI, Smart Card/CAC environment. V-ONE's SmartGate eliminates the need to individually PKI enable applications and allows you to extend PKI *across* your web and legacy applications. For many solution alternatives, integrating PKI with network, security, and operating systems requires significant modifications or even replacement of the existing systems. V-ONE's SmartGate software drops-in seamlessly with an enterprise or agency's existing network and systems infrastructure while enabling standard x.509 certificates and CACs for authentication using strong FIPS<sup>5</sup>-validated encryption and access controls.

### ***Compliance***

Many enterprises and government agencies struggle with the technical standards related to choosing and implementing a PKI solution. PKI solutions should be NIAP<sup>6</sup> compliant, including FIPS validations, and adhere to current standards. V-ONE consistently meets the latest Department of Defense certification and validation requirements in relation to PKI. Additionally, V-ONE is currently completing PKE<sup>7</sup> interoperability testing at the Joint Interoperability Testing Command (JITC), ensuring that our technology is validated for and easily integrates with each key aspect of the network infrastructure.

### ***Scalability***

Unlike many hardware-based solutions in the marketplace, V-ONE's software is easily scalable to accommodate an organization's future growth minimizing or eliminating the need for future hardware purchases or upgrades.

### ***Training and Administration***

Organizations are well aware of the training required for personnel to use and manage PKI, as well as the significant administrative burdens imposed by basic PKI requirements and processes. V-ONE technology helps you to deploy your authentication policy to secure user access, and enforce authorization rules on target applications to simplify administration and manage user access effectively. Network administrators have precise control of all users through fully configurable access permissions that can be updated, enabled, or revoked in real-time. V-ONE's patented On-line Registration (OLR) process allows users to easily register and enable their PKI credentials in less than 10 minutes, thereby allowing 1,000s of users to be enabled in a single day.

---

<sup>4</sup> GAO-04-157

<sup>5</sup> NIST Federal Information Processing Standards

<sup>6</sup> NIST National Information Assurance Partnership

<sup>7</sup> Public Key Enablement

## How SmartGate Accelerates Your PKI Implementation

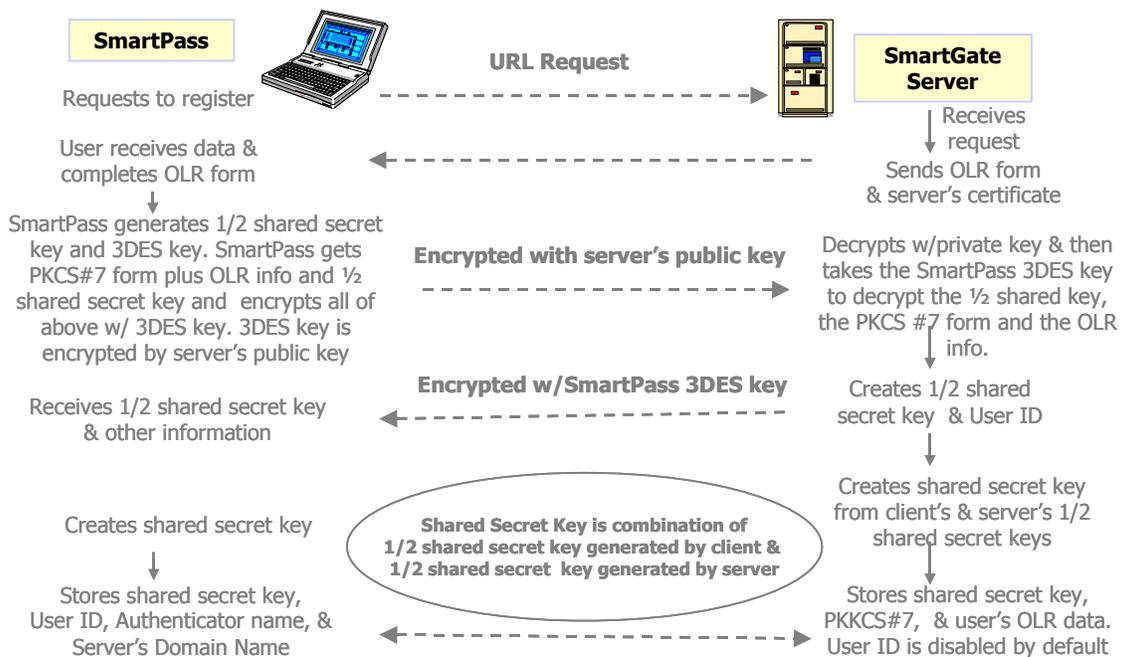
SmartGate is not a PKI, but rather a standards-based middleware solution, designed to leverage and extend existing PKI functionality. While SmartGate is not used to create or manage digital certificates, it will help you to deploy your PKI and secure access to your applications. V-ONE's SmartGate VPN (virtual private network) product includes generic PKI support, which allows it to use X.509 digital certificates for authentication.

### Establishing User Identity

The SmartPass PKI VPN client provides a list of available user profiles from the local system. PKI users must choose a PKCS #12 file (.p12 or .pfx) or PKCS #11 module and enter the corresponding access code. If the access code entered is correct, then SmartPass retrieves security information from the selected PKCS #12 file or PKCS #11 device.

PKI users then need to perform an On-line Registration (OLR) process to register to the SmartGate server (**Figure 1**). The user accesses an OLR page at the SmartGate server using their default browser and is then prompted to enter registration information as set by the SmartGate Administrator.

NOTE: Where 3DES is indicated, AES may be used instead.



**Figure 1.** On-line Registration Process with SmartGate using PKI

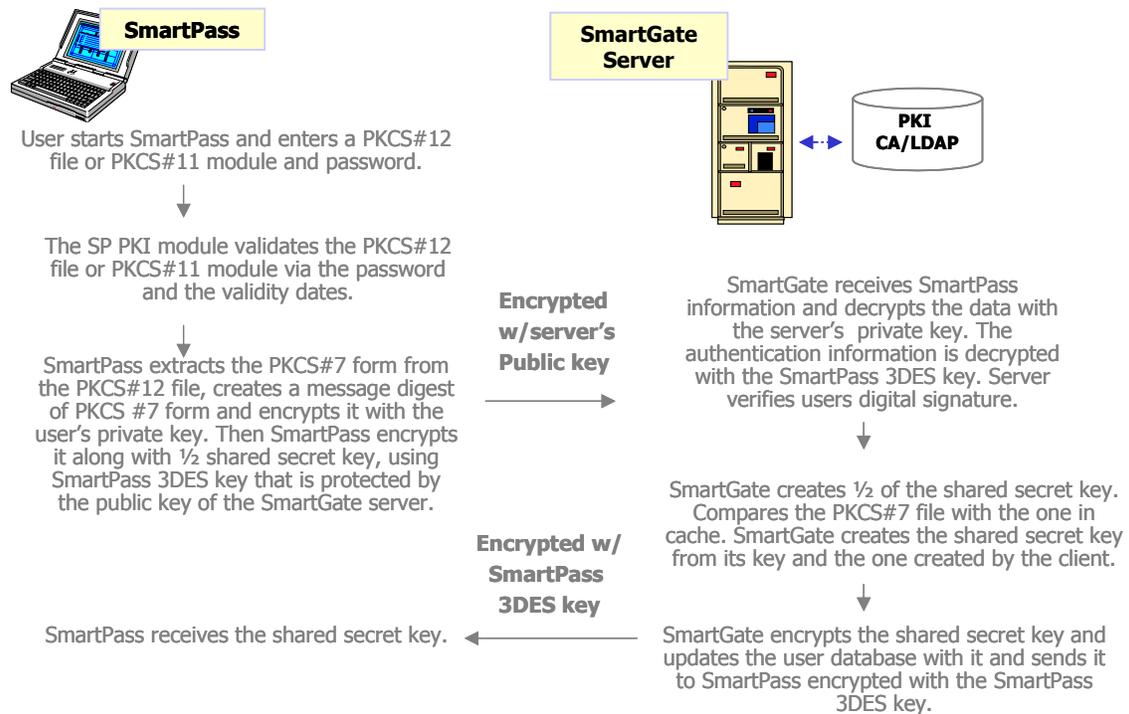
The submitted registration information is encrypted using the SmartPass 3DES key; the 3DES key is protected in turn by the public key of the SmartGate server. The registration information, PKI certificate in PKCS #7 form, and half of a shared secret key is submitted to the SmartGate server. The SmartGate server stores this information, and sends the other half of the shared

secret key along with the registration response. The SmartPass client and SmartGate server now have all of the information that they require to establish secure, encrypted VPN sessions.

Once registered, a SmartGate administrator must enable the user account, and define access rights for the user. These rights are based on both individual and group membership access controls. Network administrators may also choose to pre-configure SmartGate with predefined criteria thereby streamlining the registration process and eliminating the step of enabling users manually.

**Performing Mutual Authentication**

Once a user has registered, each time that user authenticates with the SmartGate server (**Figure 2**), the SmartPass client creates a message digest of PKCS #7 form and encrypts it with the user's private key. Then SmartPass encrypts it along with half of a shared secret key, again with SmartPass's 3DES key that is protected by the public key of the SmartGate server. The SmartGate server decrypts the data with its own private key and gets SmartPass's 3DES key to decrypt the encrypted message digest of PKCS #7 form with the user's private key. Then the SmartGate server gets a message digest of PKCS #7 form by decrypting using the user's public key. SmartGate server compares this to the one it has. If the two are the same, the SmartGate server acknowledges successful mutual authentication<sup>8</sup> to the SmartPass client.



**Figure 2.** Per session authentication process (transparent to user).

SmartGate can also provide X.509 path validation before acknowledging successful mutual authentication to the client. With the SmartGate server configured to verify Certificate Chaining, this path validation occurs. This includes signature verification, date verification, and name

<sup>8</sup> Mutual authentication is bi-directional authentication where the client is required to authenticate to the server, and the server is required to authenticate to the client.

verification of all of the certificates in the SmartGate server's encrypted database of trusted CA certificates.

Certificate Status Check can also be configured on the SmartGate server, and supports two methods of verification, CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol).

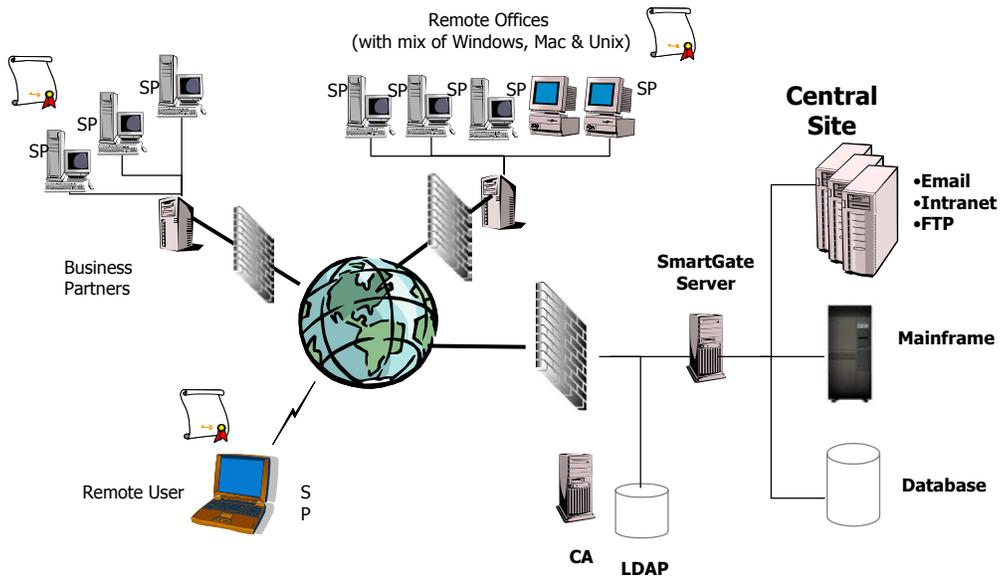
The first method involves each CA periodically issuing a signed data structure called a certificate revocation list (CRL). A CRL is a time stamped list identifying revoked certificates, which is signed by a CA or CRL issuer and made freely available in a public repository. Each revoked certificate is identified in a CRL by its certificate serial number. When a user authenticates with the SmartGate server, the SmartGate server not only checks the certificate signature and validity but also acquires a recent CRL and checks that the certificate serial number is not on that CRL. The SmartGate server periodically acquires a new CRL, based on an entry in the existing CRL.

The other method of certificate verification, OCSP, overcomes the chief limitation of CRL where updates must be frequently downloaded to keep the list current at the client end. When a user attempts to authenticate to the SmartGate server, the server sends a request for certificate status information. The OCSP responder sends back a response of "current", "expired", or "unknown".

### ***Delivering Strong Security and Valuable Benefits***

SmartGate enhances existing features of a PKI and provides new capabilities such as fine-grained access control and mutual authentication between client and server. Since SmartGate's PKI support is standards based and not tied to any one particular vendor, the ability to support overlapping PKIs removes a major interoperability roadblock.

A single SmartGate server can provide access control for an entire organization's resources (**Figure 3**). This ability alleviates the need to build and maintain access control into every application and system resource, saving both time and costs.



**Figure 3.** Sample SmartGate PKI configuration.

## **SmartGate vs. Traditional SSL**

PKI enabled security solutions that rely on browser-based SSL provide weak controls because of their loose architecture (*i.e.* the secured system has no control over the browser). SmartGate's closed architecture provides full control over the connection to the server. SmartPass and SmartGate encrypt all data using a one-time session key unique for each session. Security risks inherent in reliance on public keys are mitigated in this fashion.

In traditional SSL-based security solutions, a connection is made to the protected server before the user is asked to authenticate. It is here, at the client's browser or the application server handling access control on the trusted LAN, that most successful hacking attempts on SSL implementations occur. With SmartGate, all traffic to protected resources must authenticate to the server *before* being allowed access to the network.

## **Conclusion**

V-ONE's SmartGate product line effectively addresses PKI implementation challenges and adds manageability, viability, and scalability to PKI deployments. SmartGate's standards-based approach lends itself particularly well to situations with multiple PKIs. SmartGate provides a PKI enabled gateway with access controls and enhanced encryption based on certificates. With SmartGate technology, no user is allowed access unless it has been expressly permitted, and all access is logged.

SmartGate's PKI implementation support provides great flexibility in meeting the needs of both government and private industry.

**V-ONE Corporation**  
20300 Century Boulevard, Suite 200  
Germantown, MD 20874  
1-800-495-VONE or 301-515-5200  
FAX: 301-515-5280  
[www.v-one.com](http://www.v-one.com)

V-ONE, SmartGate, SmartGuard, SmartPass, SmartWall, and "Security for a Connected World" are registered trademarks or trademarks of V-ONE Corporation. Other company or product names mentioned in this document are registered trademarks or trademarks of their respective companies.