Exporting SmartGate's Strong Encryption Using KRAKit

SmartGate VPN Is Granted Industry's Broadest Export Approval with Implementation of V-ONE's Trusted First Party Key Recovery

June, 1999

KRAKit Description

Recently approved by the U.S. Department of Commerce – Bureau of Export Administration (BXA), V-ONE's key recovery feature KRAKit™ (Key Recovery Agent's Kit) permits customers to use strong encryption (up to 168 bits) for any application in virtually any country while enabling an organization to keep control of their own session encryption keys. This approval now enables organizations to deploy 168-bit encryption with V-ONE's SmartGate® VPN for secure communications internationally (anywhere other than the seven countries embargoed by the U.S. Government -- Iran, Iraq, Syria, Sudan, Cuba, North Korea, Libya) without the need for cumbersome third party or escrow agent key recovery processes as long as the customer agrees to manage their own keys.

For the latest information concerning U.S. encryption export policies, refer to BXA's Web site at http://www.bxa.doc.gov/Encryption/.

V-ONE enables VPNs for meaningful global electronic commerce, uniformly protected by strong encryption, while permitting customers to control their own keys – literally, the keys to all of their proprietary electronic communication.

What are the distinctions between V-ONE's Trusted First Party™, KRAKit and SmartGate?

Trusted First Party (TFP) is the name of V-ONE's key recovery methodology that allows for the re-creation of session encryption keys while ensuring that the customer always controls these keys. TFP is comprised of SmartGate, V-ONE's VPN product, along with the session key re-creation capabilities of SmartGate's KRAKit feature. This enables truly global Virtual Private Networking that offers:

- the most robust security of any key recovery or recovery-type approaches such as Private Doorbell;
- the widest global distribution allowed by the Bureau of Export Administration (BXA) – any country other than the embargoed seven;
- complete customer control of their encryption keys – there's no way for any external third parties to gain access; and,
- protection for any application in any vertical industry.

Distinguishing Feature

V-ONE's KRAKit (Key Recovery Agent Kit) product allows for the recovery, and ensures the confidentiality and integrity, of stored-shared secret keys (used for client-server authentication and creation of session keys) while allowing the re-creation of specific session keys (used to read encrypted communications.) Because of BXA's confidence in KRAKit's ability to recover session keys, V-ONE's TFP methodology does not require the storage of session keys, merely the ability to re-create them.

What is KRAKit's business case (how does it save or generate revenue)?

Acceptance of the Internet as a meaningful business resource and its enormous cost savings has been held back internationally because organizations have been averse to ceding control of their encryption keys to a third party as the price for using strong encryption across national boundaries. This reluctance can be seen by the lackluster commercial responses given to Trusted Third Party and other methods of key recovery.

Before TFP, organizations not willing to give up control of their own keys operating across national boundaries were faced with an agonizing choice – protect mission-critical data with inferior encryption or don't communicate over public networks. And, if considering a Trusted Third Party approach, they would still have to set up a costly infrastructure to secure the stored keys and face potential security risks associated with third party methods, regardless of who the third party was.

TFP enables organizations to use one strong level of encryption in one product across national boundaries while keeping control of their own keys. It opens the Internet for global business while eliminating the need to escrow secret keys and construct complicated network configurations. TFP makes possible seamless communication worldwide protected with strong encryption and customer-controlled keys with neither PKI complexity nor dedicated communications to the Trusted Third Party facility with the strong security some see lacking in session recovery approaches.

What makes this a significant improvement?

Previously, because of U.S. law relating to encryption export, SmartGate could only be used with strong encryption to establish VPNs for companies operating domestically, with their overseas subsidiaries, or in the banking/financial services sector. Now, SmartGate makes possible truly global Virtual Private Networking, with any type of company in any country (other than the seven terrorist nations), protected with strong encryption without forcing an organization to give up control of their encryption keys.

What are two or three competitors?

Trusted Third Party method – involves storing an organization's encryption keys with an external "trusted" party so that a law enforcement agency can gain access to the private data without the organization's awareness of the investigation. For most organizations, trusting a third party with their keys is not an acceptable option. Even if third party is the customer, the session key is attached to each transmission, which creates unnecessary security risks and additional overhead.

Private Doorbell – A method that enables retrieval from routers either just before outgoing messages are encrypted or when incoming messages are retrieved, assuming cooperation of the relevant network managers – managers who would have free access to all of an organization's unencrypted communications. Private Doorbell is only available for use in 44 countries, a limited selection that doesn't include important global trading centers such as Singapore and Hong Kong.

Does V-ONE's Trusted First Party approach allow the government to indiscriminately decode any message sent with the company's encryption products?

No. What distinguishes V-ONE's Trusted First Party approach is that only specifically requested keys may be re-created and that the V-ONE end customer is in complete control of the decryption keys with no possibility of third party access.

The procedures by which a legally appropriate government authority would seek to decrypt a recorded message are parallel to the way in which court-ordered wiretaps of telephones are

approved today. With the Trusted First Party approach, the same safeguards that prevent unauthorized, illegal wiretaps would be in place to protect V-ONE's customers.

Intervention by law enforcement to decrypt a recorded session with Trusted First Party would take place as follows:

1. Law Enforcement Organization (LEO) identifies suspect criminal activity.
2. LEO taps link and records sessions in question between a suspect's originating IP address and the V-ONE customer's server.
3. LEO obtains a court order for access to the subject sessions in question.
4. V-ONE Customer Administrator (not third party) responds to court order by recreating session keys for only the sessions in question using the secure KRAKit utility.
5. LEO decrypts sessions using these keys.
6. After this investigation, future sessions are private without any change in keys since none of the secure keys have been exposed.
7. It is not necessary to make the end-user aware of the intervention.

How does the recently signed Wassenaar Agreement effect encryption export and KRAKit?

On December 3, 1998, the Clinton administration announced they had persuaded 32 other countries to impose strict new export controls on encryption technology of 64 bits or longer. This agreement is a step towards leveling the playing field between U.S. and overseas encryption products. It also reinforces the fact that for strong encryption, methods of key recovery and recoverable systems will be necessary to gain approval to export.

How is V-ONE's Trusted First Party approach different from "Trusted Third Party" (TTP) systems when the TTP system is operated by the customers themselves?

Although there may seem to be similarities in comparing V-ONE's Trusted First Party approach to TTP when the customer instead of a separate agent operates TTP, there are significant differences in the systems:

- A "Key Recovery Field" (KRF) is added to every session or message under TTP systems. This field is used by the TTP to recover the session key under which the message is encrypted.
- The public key of the TTP agent is used to protect the KRF and the TTP's private key is used to access it.
- The TTP system adds complexity, processing costs and support effort to the data management and storage.

With the V-ONE TFP system, none of this is necessary, since there is NO additional key recovery data added to the protocols or storage of session keys in any system.

Does the TTP system pose possible risks to the customer's security?

It could. The private key of the TTP could become a very attractive target for the "bad guys." There are several possible attacks:

- A hacker might attempt exhaustive search of the possible keys to determine the private key.
- A bad guy could bribe a key recovery agent to get a copy of the private key.
- A key recovery agent himself could copy and use the TTP private key.

However, in any of these cases, the person with the TTP private key may be able to access ALL messages from ALL users in the domain. This access might not necessarily be obvious to any of

the operators of the system, hence they would continue to think they were operating a secure system.

If the private key is ever exposed, ALL end-users within that domain need to obtain and reload a new public key of the server in order to resume secure operations. Note that all previously sent communications have become available to the bad guys -- since the public key of the TTP protects the KRF, it is accessible if the private key is known.

Another possible risk is the invasion of client systems by virus, ActiveX or Java programs that can replace the TTP public key with a "bad guy's" public key. Thus, every message sent by the user would be protected under the bad guy's public key, not the TTP public key. This could only be detected when the TTP actually tried to use his ability to see the user's message traffic and was unable to do so.

Are there any questions of the integrity of the ability of a TTP to access data sent under the TTP scheme?

An unscrupulous individual could modify the KRF and cause the file of data to become unreadable. Because the KRF no longer is useful, there can be no TTP access to the data. Thus, a bad guy may protect his messages from viewing by modifying the KRF after the message is formatted.

Feature Matrix for Trusted Third Party, Private Doorbell, and V-ONE's Trusted First Party

Feature	TTP	PD	TFP
Can be used in any country other than the Embargoed seven nations	X		X
Can be used in important global trading centers like Singapore, Hong Kong, South Korea	X		X
Security of sessions depends on more than trustworthiness of system administrator	X		X
Logging ensures a record of when messages are read in the clear	X		X
Restriction free distribution to subsidiaries of foreign corporations	X		X
No individual Export Licensing Arrangements needed for each attempted distribution to foreign subsidiaries	X		X
No VPN modifications necessary, so no performance or overhead penalties		X	X
Customer always aware of law enforcement key recovery		X	X
No provisions for third party access		X	X
No additional key recovery field accompanies individual session		X	X
Only recorded sessions can be recovered			X

KRAKit Software Components

KRAKit Client

The KRAKit client runs as a standard Win95 (and Win98 and WinNT) application that uses SmartPass (SmartGate's client software) to secure its communications. The KRAKit client will also run on NT client machines and will eventually run on the console of an NT SmartGate server. The KRAKit client will be shipped with SmartGate 2.6.

KRAKit Server

KRAKit will run on all UNIX platforms supported by the SmartGate 2.6 server (BSDI 3.0, 3.1, and 4.0 Solaris 2.51 and 2.6, and HP-UX 10.10 and 10.20). The KRAKit Server will be included with the SmartGate 2.6 server, but will install separately.

KRAKit Administrator

The KRAKit Administrator is a Win95 (and Win98 and WinNT) application that provides organizations the ability to assign key recovery authority to chosen parties. KRAKit Administrator will not be distributed to organizations until they have returned a KRAKit end-user agreement, signed by a company officer, to V-ONE. Without KRAKit Administrator assigning KRAKit user privileges, KRAKit cannot perform key recovery.

KRAKit Pricing

There is no KRAKit license fee for end-user organizations.

How does KRAKit provide key recovery?

When users make a connection through SmartPass (see diagram below), a session key is generated to encrypt the communications through that connection (hereafter called a session). Each session starts with a "ticket" composed of a version identifier, the user ID, and some random numbers. The ticket identifies and authenticates the user and provides the key material (the random numbers) to generate a one-time session key.

The session key is created independently on both the client and the server and is used to encrypt the rest of the session. Both the client and the server have access to the user's shared secret key (it is in the SmartPass token and the server's Authentication Database). So, they can both create the same session key, independently, without actually sending the session key over the connection.

If you record a SmartGate session with a wiretap, the ticket contains the information that the server needs to find the correct shared secret key and recreate the session key. KRAKit is the application that extracts the ticket, sends it to the server, and tells the server to recreate the session key. The session key is returned and can be taken away by the LEA or used immediately to decrypt the session. Note that each use of KRAKit only recovers one session, and the user's shared secret key is never revealed.

The people who run KRAKit are called key recovery agents (KRAs). These are intended to be employees of the company that operate the SmartGate server. The KRAKit client requires two smart cards, one held by the KRA and one held by a designated security officer (a company or law enforcement official), to begin a key recovery session The idea is that it takes two responsible people to make everything work.

KRAKit is secured by SmartPass, but also has its own internal protocol that uses strong encryption and strong authentication. SmartPass is still necessary to give KRAKit access to the SmartGate system.

KRAKit Configuration Diagram