2009 Update: Remote Key Loading

Plus An Introduction to Key Bundling

July 2009

www.trustedsecurity.com

Table of Contents

Introduction

Hacks on financial networks compromising sensitive credit and debit card information continued to rise in 2008. According to a report released in January 2009 by the Identity Theft Resource Center (ITRC), there were 646 data breach incidents reported in 2008, a 47 percent increase over 2007's total of 446 breaches – a record for the most breaches in a single year. Crooks wishing to break into sensitive data networks are limited as much by their imagination as they are by the practical application of encryption and security policies used by the target network.

ATM Manufacturers have made strides to strengthen their terminals against data fraud. During the past decade, numeric pin pads were reinvented and replaced with sophisticated and secure Encrypting PIN Pads (EPP's). Now all critical encryption processes take place internal to the EPP. Today, virtually all Terminal Master Keys in ATMs are double length 3DES versus single DES. Exhaustive determination of a double length 3DES key is virtually impossible. To further strengthen keys, the acceptance of the concept of "Key Bundling" is growing. What is Key Bundling anyway? Is it necessary? We'll talk about that later in this report.

2nd Annual ATM Key Management Report:

Our goal: To share practical knowledge on ATM key management for the benefit of all companies.

Intense competition both in ATM manufacturing and financial transaction processing continues to drive a wave of consolidation across the industry. No ATM manufacturer can find safe waters to market their products, foreign or domestic. Competition is fierce. In terms of key management, how do the different ATM manufacturers stack up? For sure, one retail ATM manufacturer is making a big play to automate their ATM keying process. Who is it and who will follow?

ATM network security is a journey and not a destination. Please read on. We've reached out to a group of today's professionals who oversee this important aspect of ATM key management and security in an attempt to determine what's on their mind.

What's next for remote key loading?

Remote key loading was introduced to the ATM world at the beginning of this decade. Since then it has seen universal approval, but relatively slow adoption. Remote key enjoys wide acceptance because it is much more secure compared to traditional methods of distributing terminal master keys, as it removes the human element of handling keying material. It is also less expensive to use because with remote key loading there is no need to send two technicians or even one technician to the ATM to rekey it. Nevertheless, remote key loading is way short of being adopted on all ATM networks because it is not a simple plug and play technology. Remote key loading impacts multiple areas of the ATM network, including the ATM, the transport infrastructure, the driving host software platform, and the Host Security Module. Getting everything lined up for a smooth remote key implementation can take time.

"Even with all of the experience we have to date and the great lengths we take in preparing for installation, it is rare that we can kick back after bringing a customer up to production remote key status and say, 'Boy that was easy,'" said Dennis Abraham, President of Trusted Security Solutions. "There are many moving parts to implementing remote key loading."

> "The more preparation and thought put into implementing remote key the better. From experience we have learned that it is best to cover all the bases the best you can in advance if you want to meet or exceed your schedule."
>
> *Dennis Abraham*
> *President*
> *Trusted Security Solutions, Inc.*

ATMs have minimum hardware and software configurations that have to be met[1]. Most ATMs now have the EPP (Electronic PIN Pad) necessary for remote key loading, but having the appropriate firmware in the EPP may be another story. Additionally, the software on the ATM must meet certain minimum revision levels. Many ATM owners or processors attempting to implement remote key do not know or are unclear of what version of software or firmware is running in the ATM and EPP. This is important information to know when preparing to implement remote key.

New remote keying specific messages have been added to ATM protocols requiring the host driving software to take notice of them if they wish to support remote key loading. Some host ATM driving solutions have a version of their software that is "remote key ready". Others do not. These ATM networks are left to come up with their own solution. Then again, some host software application vendors require an upgrade to the latest version to support remote key loading and many times this can be expensive.

[1] TSS can send you a summary of what ATM manufacturers require to support remote key loading if you send a request for the same to info@trustedsecurity.com.

Please note there are multiple terms used within the industry to refer to remote key loading (RKL), including remote key management (RKM) and remote key transport (RKT).

Triton introduces remote key loading

The United Kingdom is one of the largest international markets for Triton. So when Vocalink set a date in the sand for their members to implement remote key loading, Triton took notice, as did other ATM manufacturers. Coincidentally, Triton distributors were making a lot of noise about needing remote key. "We knew that we had a deadline of April 1, 2009 to have remote key working in the UK. We met that date," said Chuck Hayes, Product Manager at Triton Systems.

Triton developers started design work on their own remote key protocol by relying heavily on ANSI X9.24 standards. Using X9.24 as a foundation, they decided to use a certificate-based process.

Triton has adeptly tackled two of the most recent challenges in remote key loading protocols. Asymmetric cryptography inherently provides for open cryptographic dialog. So to avert attacks by unauthorized hosts attempting to key an ATM, remote key protocols seek to bind the ATM's EPP to its original host. Once the EPP and host have established an asymmetric relationship, rekeys can happen freely with no limit. This is all well and good until you wish to legitimately move the ATM to a new host, such as what may happen during a bank acquisition or when an ISO wishes to move to a more cost competitive service provider. In such an event, it is common that EPPs must either be returned to a service center for recertification or receive a service call visit to have it decommissioned in the field; both of which can be costly for a fleet of ATMs. Triton has implemented the concept of integrating a unique Host ID[2] with each signed certificate released to customers in the field. By having knowledge of this unique Host ID, a relatively simple entry into the EPP key pad allows for the ATM to unbind from one host and to receive a new rekey from another authorized host.

"We knew that we had a drop dead deadline of April 1st, 2009 to have remote key working in the UK. The date is here, and we're ready for it."

Chuck Hayes
Product Manager
Triton Systems

Another improvement to some early releases of remote key protocols, which is also now included in PIN Security Council standards, is a better defense against "replay." Replay on an ATM network is an attack where an

[2] Triton has a patent pending on the Host ID concept.

opponent interferes with a cryptographic protocol and inserts part of a message that has been sent previously in a protocol inside of a new fraudulent message.

To resolve the host integrity issue, Triton instituted mandatory steps in vetting ATM owners and host processors and assigning them a unique identification used as an integral part of the protocol. Triton uses VeriSign for their certificate signing process. No certificate signing is allowed without applicants having been approved and issued a unique identification from Triton. When appropriate, Triton can arrange for this unique customer identification in the protocol to be shared or substituted by a newly issued signed certificate to another Triton customer.

Triton ATM owners desiring to use the Triton remote key protocol will need to upgrade their ATMs with the T5 EPP and R2B firmware. In addition to these requirements at the ATM, host driving platforms will have to have coded the changes required to work with the Triton remote key protocol.

A release of the Triton remote key protocol is now available in the UK. A new release for the U.S. market is targeted for mid-summer 2009. In the U.S. release, version 2.4, Triton customers will receive the remote key protocol and SSL.

"…ATM manufacturers need to get on board with a remote key protocol of their own, or be prepared to suffer the consequences in the marketplace."

Wes Dunn
Director of Business Development
Tranax Technologies

Diebold Update

Diebold continues to update their established certificate-based remote key protocol and encrypting PIN pads to increase physical and logical security in their products. In order to become compliant with the standards set by the PCI Security Standards Council, Diebold's Rupali Patel says," Diebold recently released its PCI EPP5 module which is compliant to the PCI Encrypting PIN Pad (EPP) v1.0 standard. Diebold wants to encourage and assist all customers to be compliant with all known standards issued by the PCI Security Standards Council."

Prior to the PCI EPP5 module, Diebold provided the EPP4 and later a Basic EPP5 module, both offering remote key capabilities and both compliant with the current VISA PED standard. EPP4's are grandfathered to be compliant under the PCI EPP 1.0 standards until they are either a) moved or b) they need replacing. At that time the standards call for replacement with the PCI EPP5. There is no mention in the standards of grandfathering the Basic EPP5's. Basic EPP5s are compliant from a hardware standpoint and will only need a firmware upgrade to be changed to a PCI EPP5. Any

Diebold customer needing documentation of PCI EPP certification can request one from their Diebold sales representative and they will be sent a letter of certification.

We also asked Patel about EPP serial numbers, and she said that keeping track of these EPP serial numbers is critical. "According to PCI regulations, EPP serial numbers should be tracked from cradle to grave," Patel continued. "There are multiple reasons to do this – the main point being that no unauthorized EPP should be on the network. Every EPP should have verifiable permission to be on the network."

NCR Update

NCR has released a new EPP for its new Self Serv family of ATMs. The EPP is backward compatible at the XFS level with previous PCI compliant EPPs and existing RKM implementations. Additionally, NCR now charges new customers a one-time fee for key signing. This fee covers multiple key signings and support.

In reference to keeping track of EPPs, NCR recommends its users take the time and effort to record the serial numbers of EPPs being installed in the field. NCR notes that before this transport takes place, the EPP owner should verify not just that it is loading a key into a genuine EPP, but that it is loading the key into the intended EPP. Acknowledging that keeping record of the EPP serial numbers is not needed for RKT to "work," NCR further instructs that this step is necessary for the protocol to be compliant with PCI PIN rules. NCR will provide its customers with a list of EPP serial numbers for all ATMs or kits it provides. In addition, NCR Customer Services can also now provide serial numbers of any EPP spares that may be fitted as part of a maintenance visit.

Other ATM Manufacturers

Other ATM manufacturers are gearing up for remote key as well. Wes Dunn, Director of Business Development for Hayward, California-based Tranax Technologies, said adoption of remote key loading will be critical for ISOs in the coming months. At Tranax, Dunn said they understand the importance of providing a means of remote key loading on terminals and they continue its development. Remote key loading is a hot topic and ATM manufacturers need to get on board with a remote key protocol of their own, or be prepared to suffer the consequences in the marketplace, said Dunn. Tranax expects to launch its own RKL solution by the end of 2009.

Hyosung has released a UK version of remote key that utilizes an existing RKL protocol on the market by another ATM manufacturer. They plan to release another version of remote key for the United States and other regions within the next 12 months.

Dial up versus TCP-IP in the remote key world

Roughly 90 percent of ISO driven ATMs are on dial up networks. Almost all of the current day ATM remote key installations communicate over TCP/IP networks. One would wonder if there may be a new range of challenges ahead for ISO ATM and network administrators when they first implement remote key. Here are some reasons why this is so:

- Transmission times are slower on dial up networks and remote key message sizes are much larger than usual (remote key messages can range from 2,000 bytes up to 5,000 bytes).

- Multiple calls may be required to complete a remote key loading task from start to finish. Can the ATM and the host remain in sync if multiple calls are made, particularly if an ATM user steps up to withdraw cash simultaneous with the rekey attempt?

Here is another question. How does one schedule a remote key exchange from the host-side without causing an inconvenience to a cash dispensing customer? We will wait and see how tackle this challenge on dial up networks and report back to you next year.

The building blocks of remote key loading

ATM Manufacturers vary on how much remote key capability is delivered as standard options on new ATMs out of the box. Some ATMs are delivered with remote key loading capabilities as a standard option. Other ATMs are sold absent remote key functions and the software to make them remote key capable must be purchased a la carte. Of those models that are designed to be capable of remote key loading, a buyer is wise to request assurance that it will arrive remote key ready if that is the intent.

Inspection points to check prior to implementing remote key loading include:

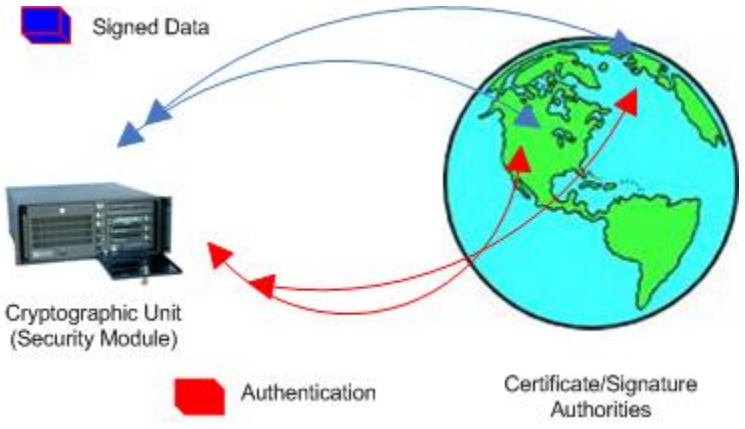
- EPPs in the ATM fleet
- ATM software levels in the ATM fleet
- Host driving software, device handlers, and security module RKT capabilities
- Procedures to secure signed certificates or signed keys for the security module

EPPs receive their cryptographic secrets necessary for remote key loading when they are originally manufactured. Firmware and configuration of the EPP, however, can differ from one ATM to another and particularly from one region of the globe to another. It is important to check with local ATM manufacturer technical representatives to confirm what is needed for EPP configuration and firmware to be remote key capable.

ATM software needs to be at minimum levels to support remote key. Check with your ATM manufacturer's technical representatives to confirm what version of the ATM software is required to be remote key capable. Then check and see what is in use in each ATM.

Host software, ATM device drivers, and the cryptographic facility all need to work in unison to support the remote key protocols desired. For example, the remote key piece could be installed and working on the host ATM driving platform, but the security module does not support asymmetric (RKT) functionality. Conversely, a cryptographic facility may be capable of handling RKT, but there are issues unaccounted for in versioning of software needed in the host, or at a particular ATM.

Finally, when an organization is ready to implement remote key for a particular ATM manufacturer, it (or its host service provider) must apply for signed certificates or keys from that ATM manufacturer. Since each vendor offering RKT uses a different CA and Root Key, the host side needs to have a signing key to be used for a particular vendor's ATMs submitted to that vendor's chosen CA for signing. This is a <u>one-time</u> need per ATM manufacturer per host security module.



When receiving signed keys for your host security module, there may or may not be a fee for this service. Check with your ATM manufacturer to see if there is one. Some ATM manufacturers run their own trust authority sites (such as NCR and Wincor) while others use a third party TA (such as Diebold [Identrus] and Triton [VeriSign]). In either case, it is common for an entity requesting signed data to be vetted through a secure channel and registered with the trust authority as well as the ATM manufacturer. Afterwards, data is generated at the user's security module specific to the desired protocol and sent to the TA. Certificates or signed keying information will then be sent back to the user for import into the security module.

"We've really come full circle on ATM key management. Nowadays, keying ATMs is almost a non-event, so why not change keys often?"

Tim Bowders
Information Security Analyst
Navy Federal Credit Union

Periodic key changes

With remote key loading techniques making it a breeze to change terminal master keys in ATMs, some ATM owners have implemented processes to change TMKs annually, monthly, or even more frequently.

Navy Federal Credit Union serves DOD personnel and their families worldwide. With branches around the globe, ATM administration was a logistical challenge. Early in the evolution of key management at Navy Federal, ATM administrators placed calls to remote branches to coach employees through the process of manually loading keys. With remote key capabilities on board, things have changed. Navy Federal not only uses remote key to install new ATMs, but they now have automated the process of periodic key changes for all their ATMs. "We set up a program where we re-key some of our ATMs each week. ATMs end up getting new keys every month," said Tim Bowders, Information Security Analyst at Navy Federal. "With our remote key server, changing ATM keys is a non-event, so why not change keys often?"

One could ask if it is necessary to change ATM master keys periodically. Are there any mandates presently known that require a frequency of changing ATM TMKs? Is there a real security advantage for changing keys periodically?

Interac[3] in Canada reportedly requires TMKs in ATMs to be changed every two years. No such requirement is known to be present today for U.S. ATM owners. The generally accepted best practice today holds that if a unique 3DES key is established in an ATM in a compliant manner and there is no evidence present of compromise to the key, then

[3] Interac Association is responsible for the development and operations of the Inter-Member Network (IMN), a national payment network in Canada.

there is no need to change the key. If on the other hand, the technology of remote key loading makes it easy to make a TMK change, why not change it as often as reasonably possible?

Remote key and compliance standards

Since remote key processes used in ATMs are still relatively new and vary from one vendor to another, criteria to measure compliant implementation of remote key loading continues to be written and fine tuned.

"Even with remote key loading reducing steps in the cryptographic key management process and eliminating much of the human intervention involved in keying ATMs, there are still some key management controls as well as controls on the management of cryptographic devices (i.e. ATM EPP, host security module) that need to be met," said Azita Amini, President of eSmart Solutions. "Those who deploy ATMs using remote key loading will have to do their homework in advance of such deployment in order to have the information they need to determine if the ATMs have been designed by the vendor to meet industry standards and compliance requirements for upcoming TG-3 (recently renamed as TR-39) and other related network audits."

The X9 Standards Committee will soon publish a new updated Section 5 to the TG-3 Compliance Guideline (now Part 2 of TR-39). This updated section deals with asymmetric cryptography used in remote Key loading. The group authoring this section felt that an updated version was needed due to the fact that the current version is too lengthy and confusing to many readers. Amini also said, "It should also be noted that the TG-3/TR-39 audit guideline and other similar audits now require ATM vendors to have gone though a periodic TG-3/TR-39 audit, as well." The vendors are then supposed to make available their remote key loading audits to their clients so that their products' compliance status is known by end-users.

Will remote key loading become a universal standard for ATM key management? It is likely so, over time. However, it is expected to be a natural and gradual evolution and not a mandated push like 3DES. Thus far, the only network known to specifically call out the use of remote key is Vocalink. The network now requires all members "to implement" remote key loading. No other network that Trusted Security Solutions is aware of has made a similar requirement of its members, nor has there been any similar directive from the PIN Security Standards Council or the X9 Standards Committee. However, with Triton adding its ATMs[4] to the league of remote key enabled ATMs, other ATM manufacturers will likely follow and the sheer numbers of ATMs able to use remote key loading could eventually cause changes in written requirements.

[4] Triton will make remote key available on their WinCE and XP units only.

Keeping track of EPP serial numbers

PCI Data Security Standards (PCI DSS) and the PCI Electronic PIN Pad Security Requirements (PCI EPP) published by the PCI Security Standards Council require ATM owners to closely monitor the inventory of EPPs in the field. To do this there must be a tracking mechanism to keep up with the EPPs across a fleet of ATMs. During remote key loading exchanges, it is common for the serial number of the EPP to be transmitted to the host. Key check values (KCV) for keys inserted in the EPP are also generally available. Therefore, it is wise for ATM owners to maintain a log of the EPP serial numbers existing in the field and the most recent KCV established in the EPP. Some remote key loading systems have such a reporting feature that will automatically log pertinent EPP and KCV information used during key loading.

PCI Security Standards Council

The PCI Security Standards Council was established by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa. The first Payment Card Industry (PCI) Data Security Standard (PCI DSS ver. 1.1) was released in September 2006 and the latest version, version 1.2 is now available on their Web site: www.pcisecuritystandards.org. On April 20, 2009 the PCI Security Standards Council announced that it was expanding its PIN Entry Device Security Requirements program to cover two new types of devices: unattended payment terminals (UPTs) and hardware security modules (HSMs). It is expected that the Council will require additional devices to be inspected in the future.

The mystery behind Key Bundling

What's all the fuss about?

Key Bundling burst onto the key management scene a few years ago amid cries of "the (cryptographic) sky was falling!" Key Bundling (KB) is not new. The earliest known implementation was in the IBM Common Cryptographic Architecture (CCA) employing Control Vectors in the 475x equipment announced in 1989. It was a side benefit of the CCA and ensured that double length DES keys could be guaranteed to have double length key properties. As a byproduct, the CCA also blocked an obscure and very complex highly technical attack which required the opponent to have the unfettered 24x7 use of the targeted system for several weeks to several months to

prepare the required input data for the attack. It was thought that it was highly likely that the system owner would notice the high system usage and determined that no intelligent opponent would attempt such an attack, opting instead for an easier and more productive approach of blackmail or bribery.

What is Key Bundling?

Key Bundling (KB) is a generic term created to avoid favoring any single vendor implementation from gaining advantage over a competitive vendor implementation by having the name of a particular vendor implementation used in any ANSI publication. Other terms are AKB, which translates into Atalla Key Block, or ANSI Key Block, depending on who is using the term. Note that the term ANSI Key Block does not appear in any ANSI approved publication. An additional term is Thales Key Scheme, and there may well be others.

What is the objective of Key Bundling?

Key Bundling (KB) is intended to prevent each "half" of a double length symmetric key, normally a DES key, from being used individually as a single length key. With today's technology, it is an accepted fact that a single length (56 bit) DES key can be found by exhaustive determination in a very short period of time. If each key "half" is individually exhausted, the "halves" could then be joined and used as a double length key. The result is the strength of the double length DES key, which when properly used and implanted, is equivalent to 2^{112} bits, is reduced to 2 times 2^{56} bits which is equal to 2^{57} bits or twice the time required to exhaust a single length key. Perhaps a few hours or less total time is required, whereas a "real" double length key is accepted as not being exhaustible by any practical means well into the future.

How well does Key Bundling do the job?

In general, a Key Management Architecture (KMA) works well if everyone would use the same KMA. Within a free market environment, there is no common KMA. Is there likely to ever be one? A few examples of KMAs are Key Variants used by Atalla, Futurex and others, as well as Thales Key Scheme (probably the most widely used), and Control Vectors used in IBM equipment. Within a given Cryptographic Domain (CD), the use of a single properly implemented and managed KMA is sufficient to ensure adequate protection of sensitive information and keys. However, very often information must be securely moved between unrelated enterprises. If both CDs implement the same KMA, the KMA provides mechanisms for the secure transfer of keys between CDs. The problem arises when information and, therefore, keys must be shared

between disjoint CDs, usually each employing a different KMA. Often there is no secure mechanism for transferring keys unless a KEK has been previously securely established through the use of key components managed under the principles of split knowledge and dual control. Using that method eliminates any guarantee that it has not been improperly loaded in a manner that permits it to be used for purposes not originally intended. That could happen due to careless or sloppy key management and policies, as well as through malicious intent. In that case, all control is lost and any protection that Key Bundling (KB) might have provided would have been nullified.

Do I hafta?

The short answer is "it depends." The only Network Operating Rules (NOR) that require Key Bundling (KB) to be implemented is Pulse. The other networks, STAR, NYCE, etc. do not require KB in their respective NORs. There are no ANSI standards that have a specific key bundling technique as a requirement. There is one ANSI Technical Report (TR-31) published that describes KB, but that is exactly what it is – a Technical Report.

The networks do require a TG-3 review to be conducted and reported in every even year. Standing alone, Technical Guideline 3 (TG-3) contains no MUSTs or SHALLs, the words defined by ANSI to delineate a REQUIREMENT, i.e. something that must be implemented if one is to claim compliance with that particular requirement. TG-3 provides a good guide and roadmap to measure the compliance and relative security of a PIN transaction system. The reason that a TG-3 must be completed every even year is the networks have written that requirement into their NORs.

What are my responsibilities?

There are no responsibilities unless an organization is connected to Pulse. In that case, one is required to develop a plan for implementation of Key Bundling. However, as of this writing, no firm date had been announced for mandatory implementation. None of the other networks have any requirements for Key Bundling other than what is mentioned in the TG-3/TR-39.

What standards apply?

As of the publication of this report, there are no standards that require Key Bundling. However, there are rumors of a pending PCI Host Security Module standard, but as of this publications, has not been issued. Remember that all standards are voluntary with no regulatory or statute muscle for enforcement. It is the Transaction Networks and

Card Service Mark owners that make the rules. However a given network may have adopted a standard and their NOR may require the implementation of certain practices as defined in the appropriate standard. When in doubt, check with your network.

Thanks to the Contributors and Reviewers

For the portion of the article concerning remote key loading, TSS wishes to thank the following contributors for their valuable input:

- Azie Amini, eSmart Solutions
- Tim Bowders, Navy Federal CU
- Wes Dunn, Tranax Technologies
- Charlie Harrow, NCR Corporation
- Chuck Hayes, Triton Systems
- Rupali Patel, Diebold Incorporated

For the section discussing key bundling, the following experts reviewed this article and made many helpful suggestions and corrections:

- Azie Amini, eSmart Solutions
- Todd Arnold, IBM
- Joe O'Connor, Pointe Consulting

About Trusted Security Solutions

Trusted Security Solutions, Inc. (TSS) is a leading provider of secure financial transaction processing solutions for ATMs. For more than 10 years, TSS technology has led the industry in innovatively addressing ever-growing ATM security and compliance demands through its secure ATM key management solutions. Serving institutions that manage cryptographic keys for ATMs, Trusted Security Solutions' A98 ATM Initial Key Establishment System ensures compliance with ANSI, ISO, and network standards. A98's patented technology has established itself as the de facto industry standard for symmetric ATM key generation and distribution.

TSS provides a module for remote key loading to accompany its patented automated symmetric key loading process so that all ATMs on a network are keyed in the most efficient and compliant means possible. TSS also provides outsourcing, consulting and training services to selected clients. Privately held, TSS is headquartered in Charlotte, North Carolina.

Trusted Security Solutions, Inc.
1500 Orchard Lake Drive
Charlotte, NC 28270
Tel: (704) 849-0036
info@trustedsecurity.com
www.trustedsecurity.com