GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Securing Sensitive Data: Understanding Federal Information Processing Standards (FIPS)

GSEC Practical Assignment
Version Number 1.4
(Amended April 8, 2002)

Thomas E. Kenworthy
July 30, 2002

Abstract

Securing and protecting sensitive data was addressed in-depth during the SANS Security Boot Camp in April 2002. During one of the evening sessions, we were examining how easy it is to sniff wireless data. BlackBerry handheld devices for remote email access are becoming increasingly prevalent in the Federal Government. Today, official guidance prohibits any wireless data networks from connecting to the wired networks. If wireless Local Area Networks (WLANs) are not allowed, then, why authorize our email to be sent over Wireless Wide Area Networks (WWANs) to these BlackBerry devices? How can the confidentiality and integrity of sensitive data be assured?

With the advent of authorized governmental use of BlackBerrys and PDAs, several questions come to mind that require research and additional explorations. First, "Why are BlackBerrys being used in the Federal Government with their official approval?" Second, "How do you determine what are "approved" hardware or software?" In this white paper, we will define FIPS (Federal Information Processing Standards), identify FIPS approved encryption algorithms, and examine some different vendor solutions and their use of these approved algorithms. What are these "approved" cryptographic modules certified under Federal Information Processing Standards (FIPS)?

FIPS PUB 140-2

We all know the importance of email in the day-to-day operations of federal, state and local government. Protecting sensitive data is especially important in today's high threat terrorist environment. The U.S. Government's standards to protect sensitive information are titled Federal Information Processing Standards or FIPS. FIPS website is http://www.itl.nist.gov/fipspubs/.

Our understanding begins with FIPS PUB 140-2, Security Requirements for Cryptographic Modules, dated May 25, 2001. Understanding how all this comes together will necessitate examining numerous other FIPS publications and validation lists. While FIPS is the official source for government users, FIPS is a valuable resource for Corporate America's data protection needs.

FIPS PUB 140-2 explains that the Cryptographic Module Validation (CMV) Program provides agencies in the Federal Government with the guidance for purchasing hardware with validated cryptographic modules. The cryptographic module vendors submit their products to independent accredited testing laboratories under the National Voluntary Laboratory Accreditation Program (NVLP) (United States, iii). The CMV Program website is located at http://csrc.nist.gov/cryptval/. This website contains links to every aspect of the CMV Program. There are links to validation lists, testing laboratories, helpful documentation, standards and their related documents and much more.

During explorations of how all these publications link together, you will notice that different FIPS publications state the following, "use of a validated cryptographic module in a computer or telecommunications system is not sufficient to ensure the security of the overall system" (United States, 1). As presented during the SANS Institute Security Essentials course, total system security is a vital concept and a FIPS PUB 140-2 validated cryptographic module is just one layer in a "Defense in Depth" solution (1-2).

This independent testing assures that the applied algorithms are indeed accurate and will protect your sensitive information. These algorithms are very complicated equations and it is vitally important that they are examined and tested to uncover any computational errors. Incorrect formulas and like incorrectly applied firewall rules will create a false sense of security.

FIPS PUB 140-2 provides the standards to be used by Federal government organizations when requiring cryptographic protection for government information protection (United States, ii). FIPS PUB 140-2 is the focal point for information confidentiality and integrity. The legal authority to publish these standards resides in public law. Additional details are in the foreword section of FIPS PUB 140-2.

Before we move on, it must be made clear that while referencing FIPS PUB 140-2, FIPS PUB 140-1 will appear both in vendor documentation and validation lists. FIPS PUB 140-2 superseded FIPS PUB 140-1. There were many changes made to the new FIPS PUB 140-2 bringing it up to date with current technologies and practices.

An exceptional publication, NIST Special Publication 800-29, "A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001", is an excellent source for more comparison details ("NIST"). One notable change is that FIPS PUB 140-2 requires an indication of when you are operating in "FIPS mode". FIPS mode means that you are using *only* FIPS approved algorithms. We will define FIPS approved algorithms during the examination of the validation lists later in this document. FIPS PUB 140-2 contains an implementation schedule and chart, but the home page clarifies usage of both standards in bold red lettering. Basically, you can continue to use FIPS 140-1 validated products after May 25, 2002. After May 26, 2002, they only accept validation reports against FIPS PUB 140-2 ("Cryptographic").

Those vendors that are in the pre-validation phase will be certified to FIPS 140-1. Therefore, you will see a few new entries into the validation list after the May 26, 2002 deadline validated to FIPS PUB 140-1. Those vendors in the pre-validation list, which was a recent addition to the web site, lets potential users and vendors obtain a current validation status. You can obtain detailed pre-validation status information at http://csrc.nist.gov/cryptval/preval.htm.

Understanding the Validation Lists

Different validation lists are available from http://csrc.nist.gov/cryptval. Your choice of a validation list really depends on what information you have as a starting point. If you want to know what certificates a particular vendor has, then check the alphabetical vendor list. There is also a list by calendar years with the tables showing certificate numbers in descending order. The higher the certificate number the more recent the certificate. This also helps you to see who has been in the business the longest, which may be of value in your vendor selection process.

The entire validation list is available in Microsoft Access database format with a template. In this database, you will find additional useful information that cannot be found on the validation list that is in the html format. This database is also key to understanding why some certificates have multiple date entries on the web site validation list. Let's pause here for a moment. It is very interesting and eye opening that so much reconnaissance information for a social engineering attack can be obtained all in one place. Full names, phone numbers, street addresses, and email addresses are available. This would be a proverbial gold mine to hackers wanting to focus on security companies. This amount of detail needs to be removed from public access. A simple link to the vendors home page would be sufficient.

First, let's examine the fields available in the FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List ("Validated").

Table 1 – Validation List Headers ("Validated")

Cert#	Vendor	Cryptomodule	Module Type	Val. Date	Level / Description

Cert# - Certificate number awarded after passing the laboratory testing procedures. A higher number means a more recent validation.
Vendor – This contains the company name as a web link if available, point of contact with an email link, phone number and Fax number.
Crypto module – Contains a link to the actual certificate, which reflects each of the Security Level ratings and an overall rating. The overall rating reflects the lowest rating found in all of the requirements areas. A link to the vendor's Security Policy and a "Validated to" are also shown.
Module Type – This will show either hardware or a software implementation.
Val Date – Validation date. When there is more than one date entered, you will find a detailed explanation of what happened on that date in the additional notes field of the Microsoft Access database form.
Level/Description – This reflects the overall level rating. This column also shows the FIPS approved algorithms used and their corresponding certificate number from

their corresponding validation list and other algorithms used, which means non-FIPS approved algorithms. The description is a short paragraph of what the module's purpose and uses are.

The Four Security Levels

Of the four Security Levels, Level 1 is the lowest level of security and incorporates at least one FIPS approved algorithm or approved security function. There are no specific physical security mechanisms required except for the use of production grade components. A Level 1 module can be executed on an unevaluated operating system. Level 2 increases the requirements by adding tamper proof evidence, authentication of an operator and execution on a trusted operation system among others. The requirements tighten in most areas in Levels 3 and 4 (United States, 12). An analysis of the FIPS PUB 140-1 and 140-2 Validation List Database, a Microsoft Access database version of the complete validation list, revealed only eight out of 220 certificates are at Security Level 4 while 101 were issued at Security Level 2. There are few vendors with products validated at Security Level 4 due to the stringent requirements ("Easter").

Understanding Requirement Areas

Inside each of the four security levels, there are 11 requirements areas. They are cryptographic module specification, module ports and interfaces, roles, services and authentication, finite state model, physical security, operational environment, cryptographic key management, electromagnetic interference/electromagnetic compatibility (EMI/EMC), self-tests, design assurance and mitigation of other attacks. FIPS PUB 140-2 provides the details on these requirements. As you progress from Security Level 1 to Security Level 4, the requirements become more stringent. For example, in the Roles, Services and Authentication requirement, it progresses from a logical separation of required and optional roles and services up to role-based or identity based operator authentication. (United States, 12)

Algorithm Basics

Before going any further, let's discuss some basics concerning algorithms. There are three main categories of algorithms: hash, private- key (or symmetric) and public–key (or asymmetric). Hash algorithms are also known as one-way hash functions because they are easy to compute, but extremely hard to reverse (if not impossible). Hash algorithms are used because any change in the data used to compute the hash causes a change in the resulting computation. Data alteration is therefore easily detectable. For example, Microsoft Windows NT uses hashes when storing their passwords. Some well-known hash algorithms are the MD5, (Message Digest) and the SHA-1 (Secure Hash Algorithm) (Mairs, 314-315). The current FIPS-approved hash algorithm is SHA-1.

As explained in FIPS PUB 180-1, the SHA-1 hash algorithm produces a 160-bit condensed representation of the message called a message digest. "The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest" ("FIPS Pub 180-1", 1)

Private-key or symmetric algorithms use the same key to encrypt and decrypt a message. This obviously simplifies key control, but you must still find a way to get the key to the person on the other end without revealing the key to the public especially when sending over the Internet. The longer the key the harder the algorithm becomes to crack (Mairs, 315). Four FIPS-approved symmetric key algorithms for encryption are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-DES, and Skipjack and AES is the FIPS-Approved symmetric encryption algorithm of choice ("Advanced"). There are separate FIPS PUBs with detailed specifications for each algorithm.

Public-key or asymmetric algorithms answer how to get your symmetric key over the Internet. The encryption provided by these algorithms is used for digital signatures and authentification purposes. The draw back with asymmetric algorithms is that they can take up to a *thousand times* longer to encrypt the same message as a symmetric algorithm. (Mairs, 318) There are three FIPS-approved algorithms for generating and verifying digital signatures: Digital Signature Algorithm (DSA), RSA (as specified in ANSI X9.31), and Elliptic Curve DSA (ECDSA; as specified in ANSI X9.62) ("Advanced").

FIPS Approved Cryptographic Algorithms

As stated earlier, the Level/Description column in the validation lists contain references to FIPS-approved algorithms and their associated certificate numbers. FIPS PUB 197 specifies the AES (Advanced Encryption Standard (AES) algorithm. FIPS PUB 46-3 specifies DES and Triple DES algorithms. FIPS PUB 81 specifies DES Modes of Operation. FIPS PUB 186-2 specifies DSA, RSA, ECDSA algorithms. FIPS PUB 180-1 specifies the Secure Hash Standard (SHS) and SHA-1 algorithm. FIPS PUB 185 specifies the Skipjack algorithm ("Advanced"). There is a separate validation list for each algorithm. You can find links to these FIPS PUBs and the validation lists for each encryption algorithm at http://csrc.nist.gov/cryptval/des.htm.

Vendor Solutions

BlackBerry

BlackBerry makes it obvious that they are approved for government uses. In a press release dated March 20, 2001, Research In Motion Limited (RIM) touts their

compliance for Federal government uses ("BlackBerry"). It states in FIPS PUB 140-2 that Federal agencies "will use" this standard when the organization specifies cryptographic protection of information. Of course, as with most Federal government policies, there are waiver procedures that can be found in FIPS PUB 140-2 (United, ii).

Let's now examine BlackBerry's claim using our understanding of FIPS. Using the vendor validation list, we find that Research in Motion was issued validation certificate number 137. Now, you can proceed to the FIPS 140-1 and 140-2 Cryptographic Module Validation list to view the details of validation certificate number 137 ("Validated"). The FIPS 140-1 validation certificate will identify the crypto module's "FIPS Mode" of operation. The FIPS approved algorithms are Triple DES (cert. #45) and SHA-1 (cert. #45). Why do they have the same certification numbers? Remember, that each cryptographic algorithm has its own validation list. It just so happens that RIM has the same number on each list. It should also be noted that there are no *other* algorithms used. Other algorithms equate to FIPS non-approved algorithms ("Validated").

How does the BlackBerry use these algorithms? The password to access the handheld device is protected by storing the actual password as a SHA-1 hash after the initial entry of the password. Every time you access the handheld, the password you enter is run through the same SHA-1 hash function and the two hashes are compared. If they match, then screen access is allowed. All data sent over the wireless network is encrypted using TripleDES. It should be noted that if you send an email to someone outside of your email domain, the data is decrypted and no longer secure. The wireless functionality of the BlackBerry handheld device provides convenient access to your email while protecting it between the handheld and the inbox/outbox of your desktop email software ("Technical", 6-7).

Prior to transmission, the BlackBerry 950 and BlackBerry 957 Cryptographic Kernel, Version 2.1, compress the plain text message and encrypts it using TripleDES. This created cipher text is transmitted over the Internet, both wireless and wired to the users PC or to the Microsoft Exchange server under the BlackBerry Enterprise Server solution. If the message is destined somewhere else on the Internet, it is sent in plain text format as with any other email system. The master key used in TripleDES is stored in flash memory using the random coordinates of random mouse movements during the initial configuration of the BlackBerry devices. The SHA-1 hash algorithm is once again applied to this 128-bit master key. This master key is only stored on the handheld device and the server. This is a symmetric key. Both the master key and session keys are zeroed if ten failed password attempts are made to access the handheld device. No information on how long the handheld device remembers failed logon attempts was revealed ("Research", 1-3).

The following summarizes the steps in the transmission of a secure email using the BlackBerry ("Research", 1-3). See Figure 1.

1. Master key generated by random mouse movements and stored as a SHA-1 hash.
2. Plaintext converted to compressed plaintext.
3. Randomly generated session key created.
4. Compressed plaintext encrypted with session key creating ciphertext.
5. Session key encrypted using the master key.
6. Cyphertext and session keys are transmitted.
7. Decryption is the reverse process.
8. Session key is zeroed and discarded.

Figure 1: Architecture using BlackBerry Enterprise Server ("Technical")
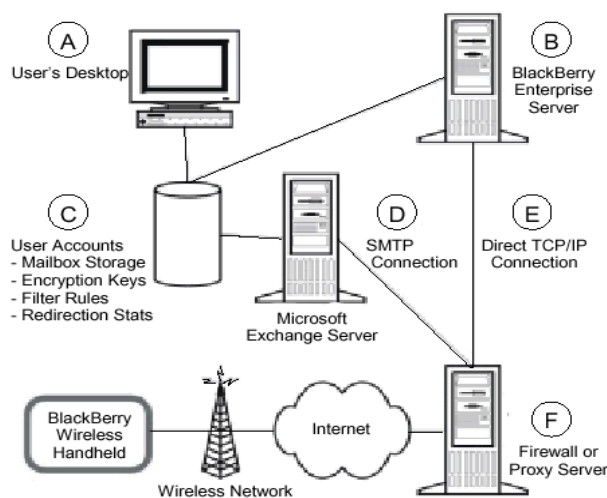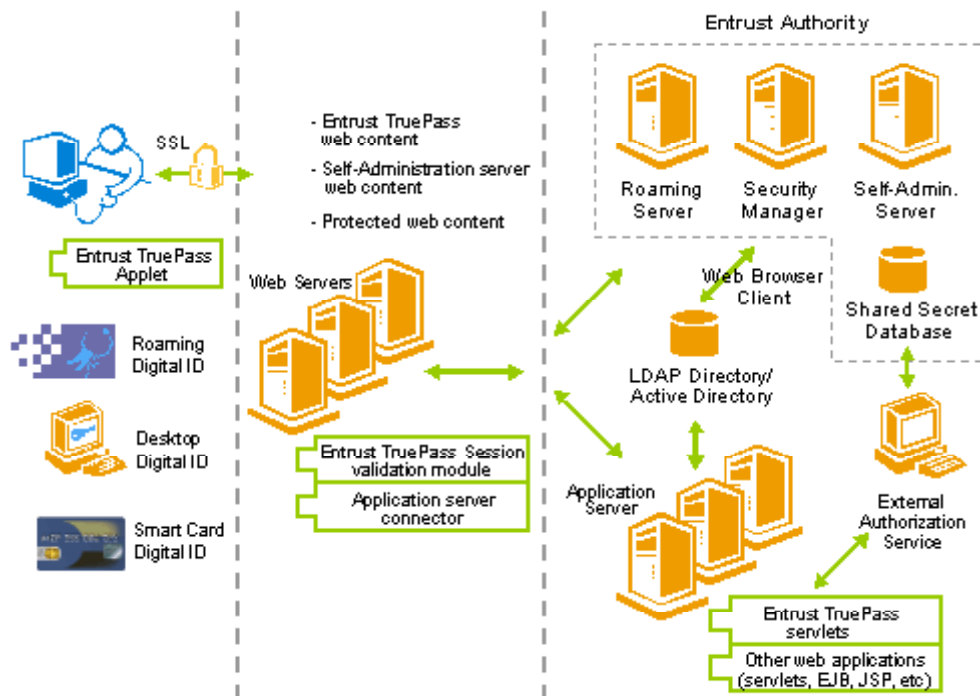

Entrust

Entrust has the most comprehensive data protection solution. Research into the vendor validation list revealed that Entrust possess 10 certificates. They are the owners of the very first certificate dating back to October 12, 1995. Certificates 1, 3, 18, 20, 85, 93, 130 and 176 are for the Entrust Cryptographic Kernel with version 6.0 as the latest version. Certificates 177 and 233 are for the Entrust TruePass Applet Cryptographic Module with version 6.0 as the latest version. The latest certificate, 233, was awarded recently on June 21, 2002 (Validated").

Both of these cryptographic modules are incorporated into Entrust's product line ("Enhanced"). The product line consists of the following:

1. Entrust Authority – PKI based security management
2. Entrust Entelligence – Security for client side enterprise applications
3. Entrust GetAccess – Single-sign-on, identification and entitlements for Web

users
4. Entrust TruePass – identification, verification, and privacy for web applications

Figure 2 – Product Portfolio Architecture ("Entrust")

Entrust, www.entrust.com, has an overwhelming amount of information covering all aspects of security whether email, web, Virtual Private Networks (VPN), wireless devices or application protection. Their security offerings are so extensive a separate white paper would be needed to cover Entrust adequately. Entrust is widely used in federal, state, local and foreign governments.

Infowave

Infowave has no overt certification, in other words, it did not submit its own hardware and software for certification. Instead, Infowave uses Certicom's security technology. There is nothing erroneous in this approach. In a February 21, 2002 press release, Infowave does indeed discuss FIPS approved algorithms and FIPS compliancy in general detail ("Read").

Based on this information, we need to see what certifications Certicom possesses that Infowave is intending to use. Using the vendor validation list, Certicom Corporation has certification's 52, 55, 59, and 67 ("FIPS"). Now, using the

Cryptograhic Module Validation List, we find that Certificate 52, CERTIFAX Fax
Encryptor CF3001, Certificate 59, CERTIFAX Fax Encryptor CF3002 and CF3003
and Certificate 67, CERTIFAX Fax Encryptor CF3102 do not apply to Infowave's
solution. (The CertiFax fax solutions allow for secure transmission and reception of
faxes using their hardware devices attached to a facsimile. However, it should be
noted for the reader that these CertiFax solutions are Level 3 certified ("Validated").

Certificate #55 is the Elliptic Curve Security Module (CLv) (Hardware version R4,
firmware version R1.4.1). This module is certified overall Level 2 with the FIPS-
approved algorithms of: DES (cert. #51), DSA/SHA-1 (cert. #19) and other
algorithms of TripleDES Encryption (allowed for U.S. Government use)
("Validated").

Infowave does use a FIPS approved algorithm, Certicom Corporation's Elliptic
Curve Security Module (CLv), but they also incorporate DESX for their symmetric
key encryption. Unfortunately, DESX is not a FIPS approved algorithm. DESX is an
improved version of DES made by RSA Data Security, Inc ("Infowave"). DESX was
chosen to improve performance. (See previous Algorithm Basics section).
Additional investigation reveals that RSA Data Security, Inc. has three certificates
from the vendor validation list: Certificate 50 (BSAFE Crypto-C Toolkit Version
4.11), Certificate 89 (BSAFE Crypto-C Toolkit Version 4.31) and Certificate 163
(BSAFE Crypto-C Toolkit Version 5.2.1) ("FIPS"). All three certificates have DESX in
the "Other Algorithms" area in the Level/Description column of the validation list
("Validated").

The diagram below (See Figure 3) shows this data flow. The data is compressed
and encrypted at the client end and sent over the wireless network, over the
Internet, then passes through the corporate firewall and into the Wireless Business
Engine ("Infowave Diagrams").

Figure 3 – The Infowave Solution ("The").

THE INFOWAVE SOLUTION — HOW IT WORKS

END-TO-END SECURITY

Data Flowing from Device to Server(s)
behind corporate firewall
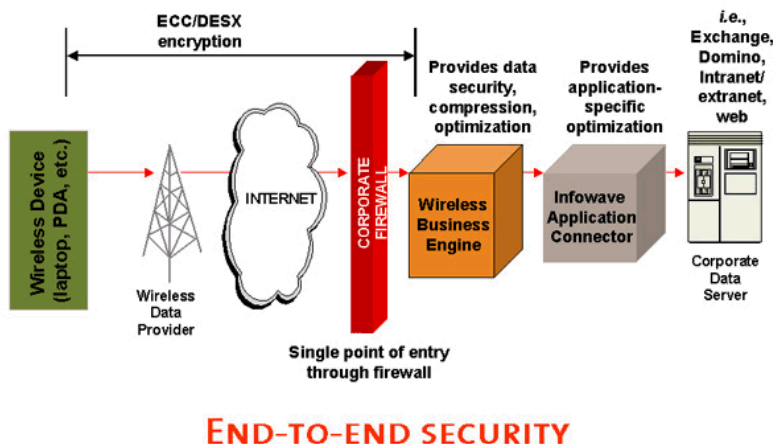
You can see that determining what algorithms are being used and where the certifications are actually coming from is more difficult in Infowave's case. Infowave's approach to protecting sensitive information does cover numerous other vendors' product lines including some BlackBerry products. Their solution is an Enterprise level solution. Again, as in the BlackBerry case, protection does not exist outside of the corporate environment. Communication with the outside world is still unprotected. Some would argue that this is not a true end-to-end solution. Due to the use of the DESX algorithm, their solution would have to waivered for Federal government uses.

Palm Handhelds

Palm is a maker of the popular Personal Digital Assistants (PDAs) hardware devices. In a white paper by Palm titled, "Securing the handheld environment – An Enterprise Perspective", Palm discusses security issues related to handhelds and their operating environments. Due to the nature of the Palm Pilot devices, numerous other vendors have applications that can be developed, installed and run on these devices. Since the focus of this white paper is Federal Information Processing Standards, an examination found that each Palm VII has a customized Elliptical Curve Cryptography (ECC) library, developed by Certicom ("Securing"). This is the same algorithm used in the Infowave solution. (See Infowave section above) FIPS compliance is already present in other products used on the Palm platform such as the V-One SmartPass VPN client for the Palm.

V-ONE Corporation, Inc. has Certificate 24, SmartPass Virtual Cryptographic Authentication Token (VCAT) and Certificate 141, SmartPass FIPS Token (Versions 4.0 and 4.1) and Citrix Extranet Client (Version 3.2) (Version 2.0)

(Validated"). The SmartPass FIPS token uses *FIPS-approved algorithms:* SHA-1 (Cert.#10), DES, TripleDES (Cert.#46) to store keys, data, and files in a single secure file on the hard disk of a personal computer, a floppy diskette, or a smart card ("Validated"). Palm also mentions, NTRU, (www.ntru.com), and their security toolkit for the PalmOS. This toolkit uses the Advanced Encryption Algorithm (AES). The Palm white paper mentions that there will be a change to FIPS that will incorporate AES in the summer of 2001. FIPS now does include AES as an approved algorithm and it is the FIPS algorithm of choice ("Securing", 7).

In another Palm white paper, "PALM: Providing Fluid Connectivity in a Wireless World", the Palm i705 handheld solution is presented ("Palm"). Palm selected the DESX security protocol, which is not a FIPS approved algorithm as described earlier during the Infowave discussion. So, as before, this solution would have to be waivered for Federal government uses.

Figure 4 - Palm i705 Handheld Solution: A secure solution for individual mobile professionals ("Palm")
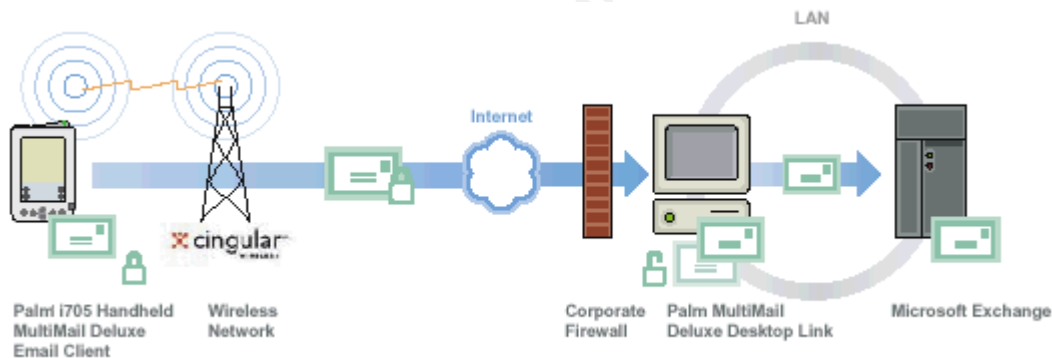
As you can see it is somewhat harder to figure out what is approved on some of the Palm devices simply due to the breadth of software applications available to run on these devices. The Palm i705 seems to be a viable solution with the exception of the choice of protocol when it comes to Federal Government uses.
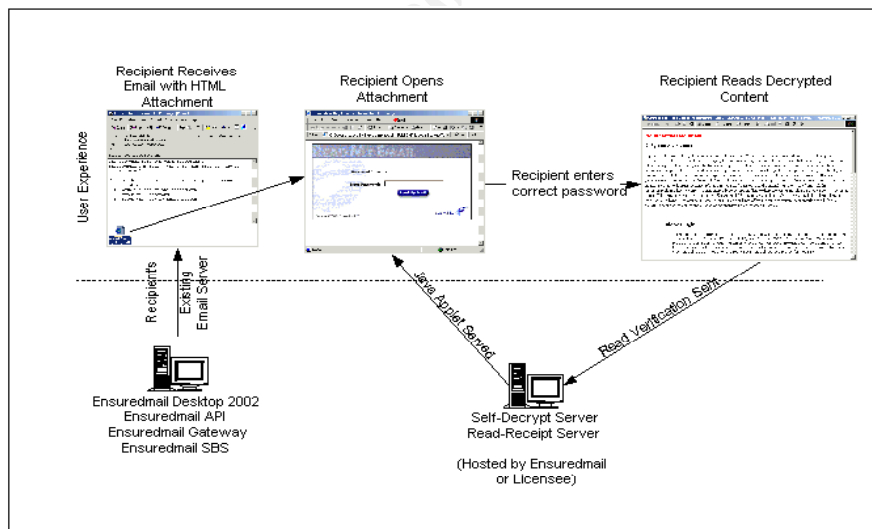
Ensuredmail

During the search for products that will protect sensitive data, a unique product called Ensuredmail was discovered. It is unique in that it runs on a personal computer and requires only an Internet connection and browser that understands Java. Ensuredmail is very vocal on their website in announcing that they have been certified to FIPS 140-1 overall Level 1. Ensuredmail uses FIPS approved algorithms

TripleDES (cert.#42) ("Triple") and SHA-1 (cert. #44) ("SHS") ("Validated'). The following is a quote from their FIPS 140-1 certification number 140. "Privacy software that: protects email, attachments, local files; supports existing email accounts; supports Microsoft Outlook; integrates with web-mail systems, provides reliable read-receipts, can prevent receipts from forwarding sensitive data" (Validated").

Ensuredmail has a nice demonstration of their software built right into their website. (www.ensuredmail.com) Ensuredmail is very easy to use and very fast. Ensuredmail uses symmetric keys so you have to get the password to decrypt the key to decrypt the message from the person with whom you are corresponding. Exchanging the password over the phone is commonly done, but in person is optimum. You can also use Ensuredmail's password hint system, which can be any hint you predetermine. If that's not possible, then use some other form of encryption mutually available, such as Steganography that hides encrypted text inside JPEG images. The details of how this is done are beyond the scope of this white paper. If you are interested in this area, there is a Steganography category in the SANs reading room. The web address is http://rr.sans.org/steg/steg_list.php. If an enterprise level solution is desired, Ensuredmail also has an email gateway called, Ensuredmail Email Encryption Gateway, an Ensuredmail Read Receipt Server and an Ensuredmail Digital Signature Module that team with your current email system.

In Figure 4, you see Ensuredmail's desktop solution to protecting sensitive data.

Figure 5 – Ensuredmail ("The Solution")

In a press release, Ensuredmail states that they were selected for use by some Air Force installations ("Ensuredmail"). Quoting an email from Mr. Fred West, Chief Operating Officer, Ensuredmail, "Eglin AFB is using it and because of them it is

also being used on a limited basis at Langley, Wright Patterson, Tyndall, Edwards, the Pentagon, Boeing and Lockheed Martin." Ensuredmail's approach of boldly emphasizing their "FIPS Approved" status is similar to BlackBerry's approach. Ensuredmail's approach however, allows a truer end-to-end solution due to the use of standard hardware and software on the client side and their hint system.

Conclusion

When checking the validation list web pages, you will notice that the last page update or last modified dates are frequently updated. The Cryptographic Module Validation (CMV) Program is a very active one. Independent testing assures that the applied algorithms are indeed accurate and will protect your sensitive information. You are now aware of what exactly "FIPS Approved" means and how to interpret and utilize the information provided by the CMV Program.

"FIPS" approved solutions are difficult to find and understand. Be assured, more solutions are coming to help protect sensitive data in today's high threat environments. Prospective security vendors should get their solutions approved through the CMV Program because certification benefits America.

References

"Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple-DES, and Skipjack Algorithms. April 17, 2002. "URL: http://csrc.nist.gov/cryptval/des.htm. (2 June 2002)

**"BlackBerry Wireless Handhelds Meet Important Security Standard for Government Customers." Press Release. March 20, 2001. URL: http://www.rim.net/news/press/2001/pr-20_03_2001-01.shtml (28 June 2002)

"Cryptographic Module Validation (CMV) Program." May 29, 2002. National Institute of Standards and Technology. URL: http://csrc.nist.gov/cryptval/. (23 May 2002)

Easter, Randall J. "FIPS PUB 140-1 and 140-2 Validation List Database." National Institute of Standards and Technology. May 28, 2002. URL: http://csrc.nist.gov/cryptval/140-1/140-1val.zip. (28 May 2002)

"Enhanced Internet Security." 2002 Entrust Inc. URL: http://www.entrust.com/products/index.htm. (28 July 2002)

"Ensuredmail selected by United States Air Force, Eglin AFB." Ensuredmail. November 19, 2001. URL: http://www.ensuredmail.com/About/press-11-19-2001.html. (16 July 2002)

"Entrust TruePass." 2002 Entrust Inc. URL: http://www.entrust.com/truepass/architecture.htm. (28 July 2002)

"FIPS 140-1 and FIPS 140-2 Vendor List." May 01, 2002. URL: http://csrc.nist.gov/cryptval/140-1/1401vend.htm. (10 June 2002)

"Government Certification". Ensuredmail. April 2, 2001. URL: www.ensuredmail.com/fips/fips.html. (12 June 2002)

"Infowave Wireless Business Engine v4.0 – Technical Overview." March, 2001. Revision 0314011. URL: http://www.infowave.com/pages/Technical_Overview_WBEv4_rev031401.pdf. (25 July 2002)

Mairs, John. VPNs: A Beginners Guide. New York. The McGraw-Hill Corporation,

"PALM: Providing Fluid Connectivity in a Wireless World." 2002 Palm Inc. URL: http://www.palm.com/wireless/ProvidingFluidConnectivity.pdf. (25 July 2002) 2002.

"Read All About It." Infowave Press Release. February 21, 2002. URL: http://www.infowave.com/pressreleases/press02-21-02.htm. (10 June 2002)

"Research in Motion: BlackBerry Cryptographic Kernel Policies." November 27, 2000. URL: http://csrc.nist.gov/cryptval/140-1/140sp/140sp137.pdf. (28 May 2002)

SANS Institute. Track 1 – SANS Security Essentials. 1.2 - SANS Security Essentials II: Network Security. 2002.

"Securing the handheld environment – An Enterprise Perspective." 2001. Palm Inc. URL: http://www.palmos.com/pdfs/securing_env.pdf. (8 June 2002)

"SHS Validation List." National Institute of Standards and Technology. July 24, 2002. URL: http://csrc.nist.gov/cryptval/shs/shaval.htm (8 June 2002)

"Technical White Paper BlackBerry™ Security." 2002. URL: http://www.BlackBerry.net/support/pdfs/bb_security_exchange_technical_wp.pdf. (28 May 2002)

"Infowave Diagrams." URL: http://www.infowave.com/trc/diagrams.htm. (25 July 2002)

"The Infowave Solution – How It Works." URL: http://www.infowave.com/trc/iwsolution.htm. (25 July 2002)

"The Solution." Ensuredmail. URL:http://www.ensuredmail.com/Business2/BusSol/reader.html. (12 June 2002)

"Triple DES Validation List." National Institute of Standards and Technology. July 17, 2002. URL: http://csrc.nist.gov/cryptval/des/tripledesval.html. (8 June 2002)

United States. National Institute of Standards and Technology. FIPS PUB 140-2 Security Requirements for Cryptographic Modules. May 25, 2001. Washington: GPO, 2001. URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. (21 May 2002).

---. ---. "NIST Special Publication 800-29 – A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2" By Ray Snouffer, Annabelle Lee, and Arch Oldehoeft. Washington: GPO. June 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf. (21 May 2002)

---. ---. "FIPS PUB 180-1 – Secure Hash Standard." April 17, 1995. Washington: GPO, 1995. URL: http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf. (28 May 2002)
"Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules (All)". July 22, 2002. URL: http://csrc.nist.gov/cryptval/140-1/140val-all.htm. (23 May 2002)