Communicating with ETMS Over the Internet: Requirements and Guidelines

Version 1.1

Prepared by the Volpe Center

6 June 2004

Background

The Enhanced Traffic Management System (ETMS) is the primary system that the FAA uses for traffic flow management. Because of this, many facilities have a need to communicate with ETMS, i.e., to send data to ETMS and/or to get data from ETMS. In the past, dedicated communication lines have for the most part been used for this communication between ETMS and a range of public and private facilities. The Internet, however, holds out the promise to greatly reduce communications cost by allowing an alternative to dedicated lines. Lowering communications cost would not only be good in itself, but it would offer the additional benefit of allowing a wider range of organizations to communicate with ETMS; this would both improve the quality of data in ETMS and also provide more users with access to that data.

Among the organizations that have a need to communicate with ETMS over the Internet are the following.

- *Airlines*: Currently airlines send in selected data to ETMS, e.g., real-time schedule updates and substitution messages. Airlines also receive various kinds of data, e.g., Airport Demand Lists, information about ground delay programs, runway visual range data, Surface Movement Advisor data, and a variety of information provided by web sites. Most airlines use private communication lines, but several airlines now use the Internet to communicate with ETMS.
- *General Aviation*: While general aviation (GA) has in the past not communicated extensively with ETMS, the trend is for more of this communication to occur, and GA increasingly needs the same connectivity as the airlines.
- *Foreign air traffic control providers*: Three foreign air traffic control (ATC) providers currently use the Internet to exchange operational data with ETMS. More are in the pipeline.
- *Others*: There has been discussion of other types of facilities gaining access to ETMS once easy Internet access becomes available. These might include FAA facilities, other federal facilities, and airport authorities.

Purpose of this Document

The primary purpose of this document is to spell out the hardware and software requirements that a facility needs to satisfy if it is to be allowed to use the Internet to communicate with ETMS. Another purpose is to provide practical guidance on how to proceed to achieve this connectivity. As mentioned above, several organizations already use the Internet to communicate with ETMS. In setting these organizations up to communicate with ETMS over the Internet, we have learned what works, what is easy, what is hard, where the pitfalls are, and how to avoid them. The lessons that have been learned in providing this access are embodied in this document.

Design Goals

In devising a solution that a facility can use to communicate with ETMS over the Internet, three design goals have been adopted.

- **Cheap***:* The motivation for using the Internet is to save the cost of expensive dedicated communications lines, so the solution must be cheap if it is to be of any interest.
- **Secure***:* Since ETMS is an operational FAA system, security of ETMS is necessary. A solution is considered secure if it meets the following criteria.
  - *Authentication*: If a facility connects to ETMS, each side needs to be sure that the other side is who it claims to be and not an impostor who seeks to steal or to corrupt data.
  - *Confidentiality*: If a transmission is stolen (as it easily can be if the Internet is used), then the thief should not be able to read the transmission.
  - *Integrity*: If a transmission is intercepted and changed (as it easily can be if the Internet is used), then the recipient must be able to recognize this tampering and discard the transmission.
- **Easy***:* Clearly, the easier it is to set up and maintain a solution, the better that solution is.

The Solution

The FAA has selected the use of a virtual private network (VPN) as the solution that meets these design goals. We will not go into a detailed description of VPNs here, but the essence of a VPN is that every transmission is encrypted, where the encryption is strong enough that for practical purposes it is unbreakable.

Sometimes the analogy is drawn between a VPN and a tunnel. One can envision a tunnel with impenetrable sides that extends from the facility to ETMS, where the impenetrable sides are provided by the VPN. This tunnel allows the facility and ETMS to communicate in safety while avoiding the thieves, hackers, and troublemakers who infest the Internet.

How does a VPN meet the three design goals? Consider the three security criteria.

- *Authentication*: Since an impostor does not have the encryption key, any impostor can be recognized, and his or her attempts to connect can be rejected.
- *Confidentiality*: If a thief steals a transmission, the thief cannot read it since he or she cannot decrypt it.
- *Integrity*: If a hacker changes a transmission, the VPN builds in the ability to detect the fact that this transmission has been changed, and it is then logged and discarded.

Cheapness is achievable because the Internet is used and because competition has driven down the cost of the needed software and hardware. A VPN can be readily set up if a facility has a security expert; if not, then it is not be cheap and easy.

How to Implement the Solution

Suppose that an organization has been approved to communicate with ETMS. For example, suppose that an airline or GA data provider has been approved to participate in the Collaborative Decision Making (CDM) Program. The organization that has been approved, which for the rest of this document is called a user, needs to do the following.

- *Acquire VPN software:* This is the software that creates the VPN, or the tunnel referred to above.
- *Acquire firewall software:* This is the software that provides the firewall functionality, which is needed to complete the security of the environment. (It might be that the VPN and firewall software are integrated, so it is only one software package that must be acquired by the user. Also, the user might already have suitable VPN or firewall software.)
- *Acquire hardware to run the VPN and firewall software:* Hardware is needed to run whatever VPN and firewall software the facility has selected.
- *Set up the VPN and firewall software:* That is, install the VPN and firewall software on the hardware, and configure the software so that it will communicate with ETMS.
- *Install the application software.* Install the software that will send data to ETMS or fetch data from ETMS. Exactly what is installed will depend on the needs of each user.
- *Maintain the VPN and firewall software:* Over time it will be necessary to upgrade the software, apply security patches, replace failed hardware, reconfigure the software, or do any number of other things to keep the VPN running.

The rest of this document provides the requirements that a user would need to follow, and it also provides guidelines and tips.

Technical Requirements

The user must satisfy five technical requirements to be allowed to connect to ETMS over the Internet using a VPN.

1) The user's VPN gateway must have a fixed, Internet-addressable IP address.

2) The user must install VPN software that complies with the IPSec standard. The VPN must support:
   a) IPSec / IKE Authentication: Pre-shared secret and digital certificate
   b) Encryption: 3DES and AES
   c) Authentication: MD5 and SHA-1

3) The user must install a firewall that will protect ETMS and the user network from the Internet. This firewall must have the following properties.
   a) It must have a written security policy that is implemented. This security policy must allow only the approved traffic to go to ETMS. The security policy must be granular enough to specify source IP address, destination IP address, and ports.
   b) The firewall must protect the VPN. That is, the firewall must be between the VPN gateway and the Internet.
   c) The firewall must keep logs that store enough data to analyze a potential attack. These logs must also show detailed data on connection attempts and VPN negotiations.
   d) The firewall must employ stateful inspection and not just do packet filtering.

4) The user must run the VPN and firewall software on a machine that runs a secured and hardened operating system.

5) The user must maintain the VPN, firewall and operating system software at a currently supported version and apply all appropriate system and security patches.

Elaboration of the Technical Requirements

The statement of the requirements in the previous section has been kept short and concise to prevent confusion over what the requirements are. This section adds explanation to help the user understand these requirements.

The VPN gateway is the machine that runs the VPN software. When the VPN is established, ETMS will see an IP address for this machine. The first requirement says that ETMS must always see the same IP address. The problem is that sometimes an internet service provider (ISP) will dynamically assign an IP address when a connection is made; if this were to occur, then ETMS would see a different IP address every time a connection was made. This cannot be allowed for security reasons. It is the responsibility of a user to have a single, public IP address that ETMS will always see when a VPN connection is made. (Exception: If for redundancy a user wants to use two addresses, this is allowed, as long as these addresses are known and fixed. What is not allowed is the address being dynamically chosen from a large set of addresses.)

IPSec, which stands for Internet Protocol Security, is a set of IP extensions that provide security services. Software being compliant with the IPSec standard, in short, is what provides the VPN functionality. The second requirement, then, is that the user runs VPN software that complies with the IPSec standard. IPSec allows many different options that affect the level of security that is achieved, and this requirement also specifies the options that the user's system must be able to support.

The third requirement is that the user must have a firewall. In particular, this requirement is designed to rule out using a router to run the IPSec-compliant software. Firewalls go beyond routers in terms of logging, management, and flexibility of security policies. The extra security of a firewall is required.

The fourth requirement is that the user runs a hardened operating system, which means that unneeded portions of the operating system have been removed, and the remaining portions are configured to improve security. Experience shows both that hardening is essential to maintaining a satisfactory level of security and also that it can be complicated. Since the hardening that should be done is very dependent on the specific operating system, no attempt will be made here to spell out what must be done. See the appendix for web sites that provide useful information on how to harden a system. NOTE: The use of an appliance with a pre-hardened operating system will meet this requirement.

The fifth requirement, which is to keep the VPN and firewall software current, is necessary to maintain appropriate security. This requirement is most easily met by using an integrated appliance, as upgrades and patches are released as a bundle by the vendor. See the appendix for useful web sites.

Guidelines for Users

There are a host of ways that a particular user could go about meeting the requirements, and a user new to VPNs might find the array of choices confusing. Therefore, this section presents examples of products that a user might select, and this has two advantages:

- This explicitly shows a user what products could be purchased that would allow the user to meet the requirements.
- This shows products that are known to be compatible with the IPSec-compliant software used on the ETMS end.

The second point is important since it can often be difficult to get one vendor's implementation of IPSec to interoperate with another's. What this means is that if the user chooses some random IPSec-compliant software, it might not run with the CheckPoint IPSec software that ETMS uses, or, more likely, it might take a great deal of work to make the user software interoperate with the ETMS software. It must be stressed that interoperability of any IPSec-compliant software with the ETMS infrastructure cannot be guaranteed. If a user follows the choices given here, this will greatly speed up the process of getting connected. If the user elects to choose some other configuration, this could lead to significant extra work for both the user and Volpe, and this could greatly slow down the process of getting connected.

Consider first the software and then the hardware. Throughout, we will describe the experience that Volpe has had with these products over the last three years; this should be thought of as tips for the possibly inexperienced user rather than as recommendations.

The specific products mentioned below are only examples of products that would allow the user to meet the technical requirements. The remarks concerning products should not be construed as recommendations, and there is no requirement to use these particular products.

VPN and Firewall Software

On the ETMS end, CheckPoint VPN and firewall software is used. Over the years Volpe has found the CheckPoint software to be excellent in terms of security, performance, reliability, and cost-effectiveness. An example of a software product that a user might employ to meet the security requirements is CheckPoint Express, which provides the firewall, VPN, and management software. In particular, the following specific products would be appropriate.

	Check Point Solution	**Approximate price**
1	**CPXP-SC1-50-NG;** Check Point Express 1/50. Includes SmartCenter Express management for 1 site, one VPN-1 Express Gateway protecting 50 users and SecuRemote.	$ 2375
1	**CP-ENT-SS;** Check Point Enterprise Software Subscription for Express 1/50, for one year.	$ 500
	CP-ENT-GS; Check Point Enterprise Standard Gold Support for Express 1/50, for one year.	$ 500

For more information about these and other, more capable CheckPoint products, see CheckPoint's web site at www.checkpoint.com/products/connect/smalloffice.html

One caution about this software (or any VPN software) is needed. Volpe has found that installing and configuring the VPN software requires considerable experience. If someone comes to this problem fresh, even a person with considerable IT experience, it could take weeks or perhaps months to get up to speed and to set up the system. While Volpe will consult with users to help them, Volpe cannot take on the responsibility of setting up the VPN software for users. Therefore, if a user does not have in-house personnel with experience in this area, the user should consider hiring a consultant to set up the software and give a tutorial on how to maintain it. Volpe has found that once the software is set up, it is easy to maintain, but setting it up is a hard job that should not be underestimated.

Once a CheckPoint-to-CheckPoint VPN has been set up, Volpe's experience has been that the VPN functions flawlessly, and it is easily monitored and controlled.

Hardware

If the user decides to go with the CheckPoint software described above, then the user will want to use hardware that CheckPoint has certified to be compatible with this software, which includes the following platforms.

- Advantech
- Barbedwires
- Celestix
- Intrusion
- Linux
- Nokia
- SecurePlatform
- Solaris
- VPN Dynamics
- Windows

For further information on these platforms and for a current list, see CheckPoint's web site at:
www.checkpoint.com/products/connect/smalloffice_sysreq.html
www.checkpoint.com/products/choice/platforms/platforms_software.html

The user will perhaps want to pick from the list of certified platforms some platform with which the user's IT staff has experience. For example, if the user has experience with Intel PCs running Windows, this would provide a low cost, easy-to-deploy platform. The major disadvantage to this approach is that the responsibility for hardening the operating system and for making on-going security patches is the responsibility of the user. If an IT team were already doing this security work for other systems in the network, then this might be the best choice.

Integrated Solution

If the user's IT staff does not have experience with firewalls and VPNs, then the best choice might be an appliance that integrates a hardened operating system with the firewall and

VPN software. In particular, one brand of hardware that Volpe has had very good experience with that provides an integrated solution is Nokia. A Nokia system integrates the hardware with the VPN software, firewall software, and hardened operating system. For concreteness, we will give some information about one such appliance for a user seeking an inexpensive solution.

		Nokia IP 130 and CheckPoint Express Solution	Approximate Price
1	1	**NBB0130000;** Nokia IP130 Base System Bundle. The base bundle includes a Nokia IP130 with 256MB memory, three integral 10/100 Ethernet interfaces, on-board encryption accelerator, power cord, Nokia routing software – strong encryption, and system documentation.	$ 1175
2	1	**NSP5002130;** Nokia Access 5x8 Support for IP130, 1 year contract.*	$ 350
3	1	**CPXP-SC1-50-NG;** Check Point Express 1/50. Includes SmartCenter Express management for 1 site, one VPN-1 Express Gateway protecting 50 users and SecuRemote.	$ 2375
4	1	**CP-ENT-SS;** Check Point Enterprise Software Subscription for Express 1/50, for one year.	$ 500

* The Nokia Access support includes technical support for Check Point.

Volpe has found the Nokia appliances to be a stable, mature platform. They offer VRRP fail-over, integrated routing, a hardened operating system, and software updates that can be installed via FTP. Nokia has solid technical support and a good track record with CheckPoint products. In particular, the Nokia appliances present an especially easy solution to the problem of how to update the software as, e.g., security patches are issued. For the Nokia, if you can FTP, then you can quickly apply security patches.

NOTE: These products are available as this is written in May 2004. This is a very fast moving area, however, and it should be expected that there will be rapid turnover of products.

How To Get Connected to ETMS

If you are interested in connecting to ETMS using a VPN, the first step is to contact the FAA to get a copy of the memorandum of agreement you need to sign. The second step is to contact Volpe to discuss your situation and determine specifically what you need to do.

FAA contact: Tim Grovac, (703) 9094-4402, tim.grovac@faa.gov
Back-up FAA contact: Charles Vomacka, (703) 925-3113, charles.vomacka@faa.gov

Volpe contact: Rick Oiesen, (617) 494-2309, oiesen@volpe.dot.gov

Summary

This document has spelled out the requirements that a user must meet if it is to be allowed to connect over the Internet to ETMS. It is important to distinguish between the requirements and the guidelines. The five requirements must be satisfied, while the user is free to ignore the guidelines. The user should recognize, however, that setting up a VPN can be a complicated process, and this process will be eased if the guidelines are followed. If a user follows these guidelines, this might well save both the user and Volpe a lot of time and trouble, and this will minimize the time until the user's VPN is operational. If, however, for some reason, such as equipment already in place or expertise on the user's staff, the user does not want to follow the guidelines, it is still necessary to meet the requirements, which are the bare minimum that is necessary if a user is to be allowed to use a VPN to communicate with ETMS.

Appendix: Hardening the System

The hardening of the machines that run the VPN and firewall software is the responsibility of the user. Below are links that provide information on how to accomplish the system hardening.

Windows Based systems:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315669&sd=tech
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/lockguide.asp
http://www.labmice.net/articles/securingwin2000.htm
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2kprocl.asp

Linux Based Systems:

http://www.arsc.edu/~lforbes/cug/HHPaper.html
http://www.linuxsecurity.com/resources/server_security-1.html
http://www.linuxworld.com/linuxworld/lw-1999-05/lw-05-ramparts.html
http://www.linuxsecurity.com/docs/LDP/Security-HOWTO/
http://www.linuxsecurity.com/docs/LDP/Security-Quickstart-HOWTO/

General Security Information:

http://www.cert.org