DATA SURETY DEMONSTRATIONS

Tim Draelos, Mark Harris, Pres Herrington, and Dick Kromer
Monitoring Technologies Department
Sandia National Laboratories

Sponsored by U.S. Department of Energy
Office of Nonproliferation and National Security
Office of Research and Development
Contract DE-AC04-94AL85000

ABSTRACT

The use of data surety within the International Monitoring System is designed to offer increased trust of acquired sensor data at a low cost. The demonstrations discussed in the paper illustrate the feasibility of hardware authentication for sensor data and commands in a retrofit environment and a new system and of the supporting key management system. The individual demonstrations are summarized below.

- *Demonstration of hardware authentication for communication authentication in a retrofit environment.*

Data authentication at the sensor is not required for existing installations until a planned upgrade is performed. Until that occurs, communication authentication is recommended at the earliest convenient point before the external communications interface at the station. We have demonstrated a low-cost solution to add digital signatures to all data channels in the existing Alpha protocol data stream at a station. Commercial off-the-shelf hardware is used (Sun SPARCstation with a FORTEZZA card). A simple command authentication system using the proposed command message format was also demonstrated.

- *Demonstration of hardware authentication in a new system.*

For new installations, data authentication is required at the sensor. At the Symposium, we will demonstrate a low-cost solution to sign all data channels at the remote digitizers of the DOE Prototype Infrasound Array at Los Alamos, NM. Commercial off-the-shelf hardware is used (FORTEZZA card). A command authentication system using the proposed command message format was also demonstrated.

- *Demonstration of key management for sensor data and command authentication.*

Demonstration of a proposed IMS key management system included the following elements:

1. IDC private/public key pair generation and public key distribution
2. Sensor private/public key pair generation
3. Sensor public key acquisition/registration
4. Sensor public key certification
5. Sensor public key certificate distribution and verification
6. Sensor private key and public key usage
7. Remote sensor key updates

In particular, the demonstration illustrates the simplicity of daily IMS personnel tasks necessary for proper and secure management of keys.

Key Words: Authentication, Key Management, Infrasound, Sensor, Upgrade

DISCLAIMER

DATA SURETY DEMONSTRATIONS

OBJECTIVE

The implementation of data authentication within the International Monitoring System (IMS) is scheduled to begin in calendar year 1999. The objective of this work was to clarify the specifications recommended in ***Task Leader Guidelines on Authentication (CTBT/PC/III/WGB/TL/52/Rev1 and CTBT/PC/V/WGB/TL/92)*** [1, 2] and determine the impacts that these specifications will have on present and planned monitoring stations. Although each demonstration targeted a specific area, some specifications were common to all.

RESEARCH ACCOMPLISHED

Common usage of the term "data authentication" implies a mechanism to verify the authenticity and integrity of electronic data. Application of this mechanism provides assurance that the source of the data and the data have not been modified since the application of a "digital signature". A digital signature is a bit stream appended to a message which establishes for the recipient the source and integrity of that message. The Digital Signature Algorithm (DSA) was recommended for the IMS. In this approach, the private key is known only to the data collecting sensor system (so impersonation is not possible) and certified public keys (associated with that unique private key) are distributed to all authorized data users.

Demonstrations were carried out in three areas of concern regarding the likely requirements for data authentication at IMS stations and the associated task of managing the private and public keys required for authentication.

Demonstration of hardware authentication for communication authentication in a retrofit environment.

The implementation of data authentication within the International Monitoring System (IMS) is scheduled to begin in calendar year 1999. According to the Task Leader Guidelines on Authentication (CTBT/PC/III/WGB/TL/52/ Rev1) [1]: "For existing stations, authentication should be implemented at upgrading. When upgrading is substantially delayed, communication authentication is recommended by authentication at the earliest convenient point before the external communication interface."

Data Communication Authentication

A system has been developed at Sandia National Laboratories to demonstrate communication authentication. This system provides an example of a cost effective solution to authenticate all data channels in an existing Alpha protocol data stream at a station. The demonstration system consists of a Station Authenticator, our model for the authentication equipment at the station, and an NDC Simulator that is used to monitor authentication performance (Figure 1). The Station Authenticator consists of commercial off-the-shelf hardware (Sun SPARCstation 5 with a FORTEZZA card) running commercial and custom software.

In this system Alpha data is sent from the existing station equipment to the Station Authenticator, where it is signed and forwarded to the NDC. The standard Alpha protocol is used with the exceptions that a signature frame count is inserted in the station specific bits of the status field of the Channel Sub-Frame, and the description fields of the Data Frame are used to communicate key change information. All data channels are signed using the same private key by a single FORTEZZA card.

Command Authentication

Most stations in the IMS will be capable of receiving remote commands for the purpose of system maintenance and calibration. Untimely execution of these commands could adversely affect data quality and IMS performance could be degraded by a coincidental action at a set of stations. To minimize this threat, external commands to IMS stations are required to be signed at the point of origin and verified at the stations.

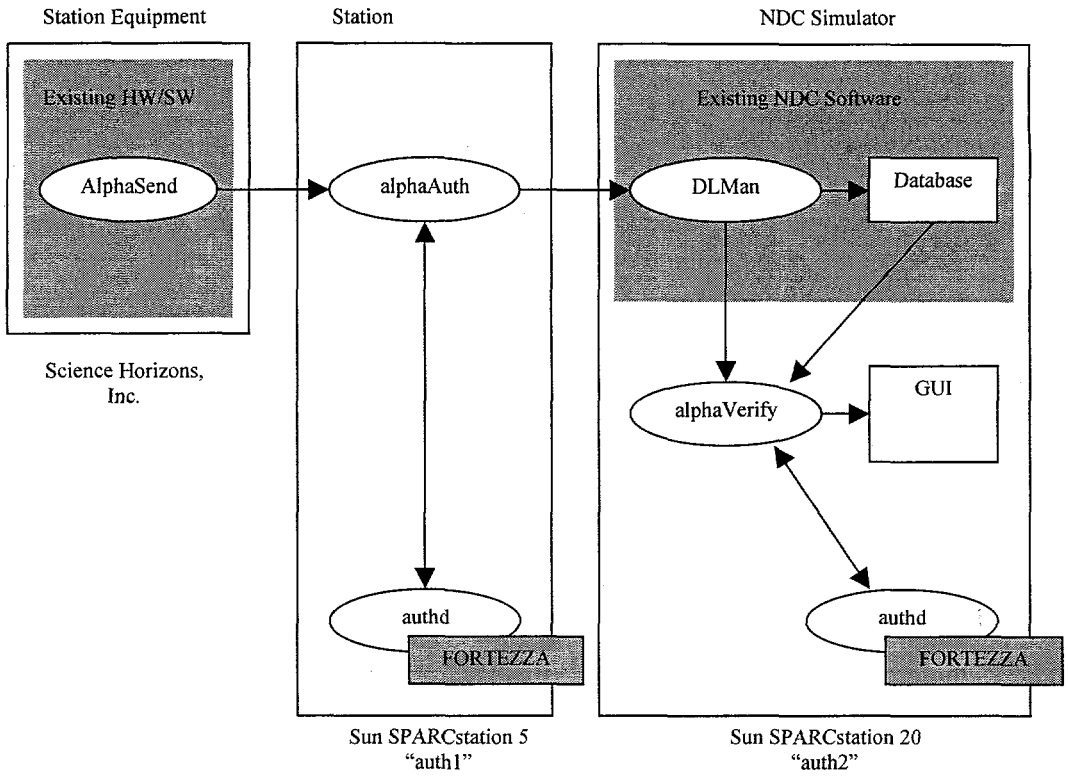

Figure 1. Data authentication system overview. Alpha protocol data flows from the Station Equipment (AlphaSend) to the Station Authenticator (alphaAuth) to the NDC Simulator (DLMan). The Station Authenticator and NDC Simulator are installed on the station LAN.

A command authentication system using the proposed command message format [3] was developed for this demonstration. This software consists of a command formatting tool that is run on the NDC Simulator and a command receiver which runs on the Station Authenticator (Figure 2).

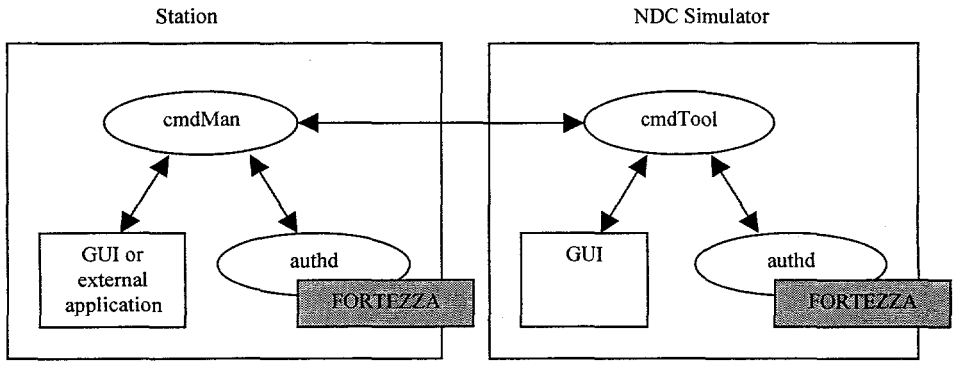

Figure 2. Command authentication system overview. The Command Tool (cmdTool) on the NDC simulator is used to enter a command for a station and channel. The Command Manager (cmdMan) on the Station Authenticator receives the command, verifies the authentication signature, and processes it for the station.

The Command Tool provides a GUI which allows selection of the destination for the command (station and channel) and setting of the command message (Figure 3). It formats the complete command message, signs it (using authd), and sends it to the command receiver via a socket connection. The command receiver verifies command authenticity and sends an acknowledgment to the Command Tool.

Command authentication requires that each command receiver maintain the public key for all authorized command originators. Depending upon the station equipment, command receivers may include each sensor and/or the station hub. Command originators may include the IDC and appropriate NDC.

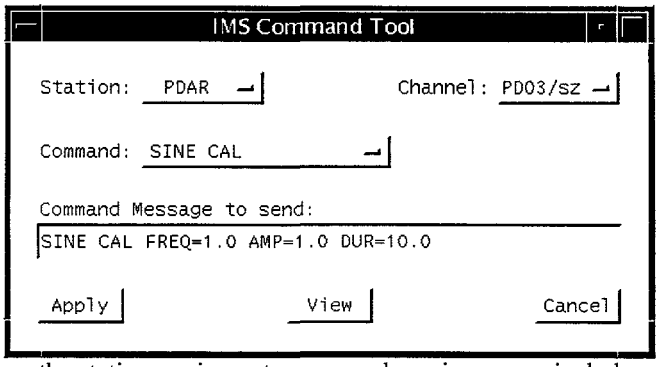

Figure 3. Command Tool graphical user interface.

Pinedale Demonstration

This system was demonstrated at the existing IMS primary station, PDAR, at Pinedale, Wyoming, during August, 1998. The Station Authenticator and NDC Simulator were installed at Pinedale and received Alpha data from the RPC. This exercise demonstrated all of the required characteristics of authentication in a retrofit environment as follows:

- Initialization of the Station Authenticator FORTEZZA card using the certification laptop computer
  - Generate new DSA keys on the FORTEZZA card
  - Install the new public key in the NDC Simulator
  - Install the FORTEZZA card in the Station Authenticator
- Normal operation of the data authentication equipment
  - The station equipment sends Alpha protocol data frames to the Station Authenticator
  - The Station Authenticator signs the data frames and forwards them to the NDC Simulator
  - The NDC Simulator verifies the digital signature and displays the results
- Error detection by the authentication equipment
  - Insert bit errors into the signed data frame, confirm that the NDC Simulator does not verify the frame
  - Change the public key in the NDC Simulator, confirm that the NDC Simulator does not verify the data frames
  - Change the key in the Station Authenticator (switch the FORTEZZA card), confirm that the NDC Simulator does not verify the data frames
- Command authentication from the NDC Simulator to the Station Authenticator
  - Send signed command messages from the NDC Simulator to the Station Authenticator using the IMS Command Tool, confirm that the station verifies and logs the command and acknowledges it to the NDC Simulator
- Remote key change in the Station Authenticator
  - Send key change command from the NDC Simulator to the Station Authenticator using the IMS Command Tool
  - Confirm that the public key on the NDC Simulator is updated (via an Alpha Data Frame)
  - Confirm that Alpha data frames continue to verify at the NDC Simulator using the new key

Demonstration of hardware authentication in a new system.

According to the Task Leader Guidelines on Authentication (CTBT/PC/III/WGB/TL/52/Rev1) [1]: "For new installations and equipment upgrades after 1998, data should be authenticated at the first point in the acquisition

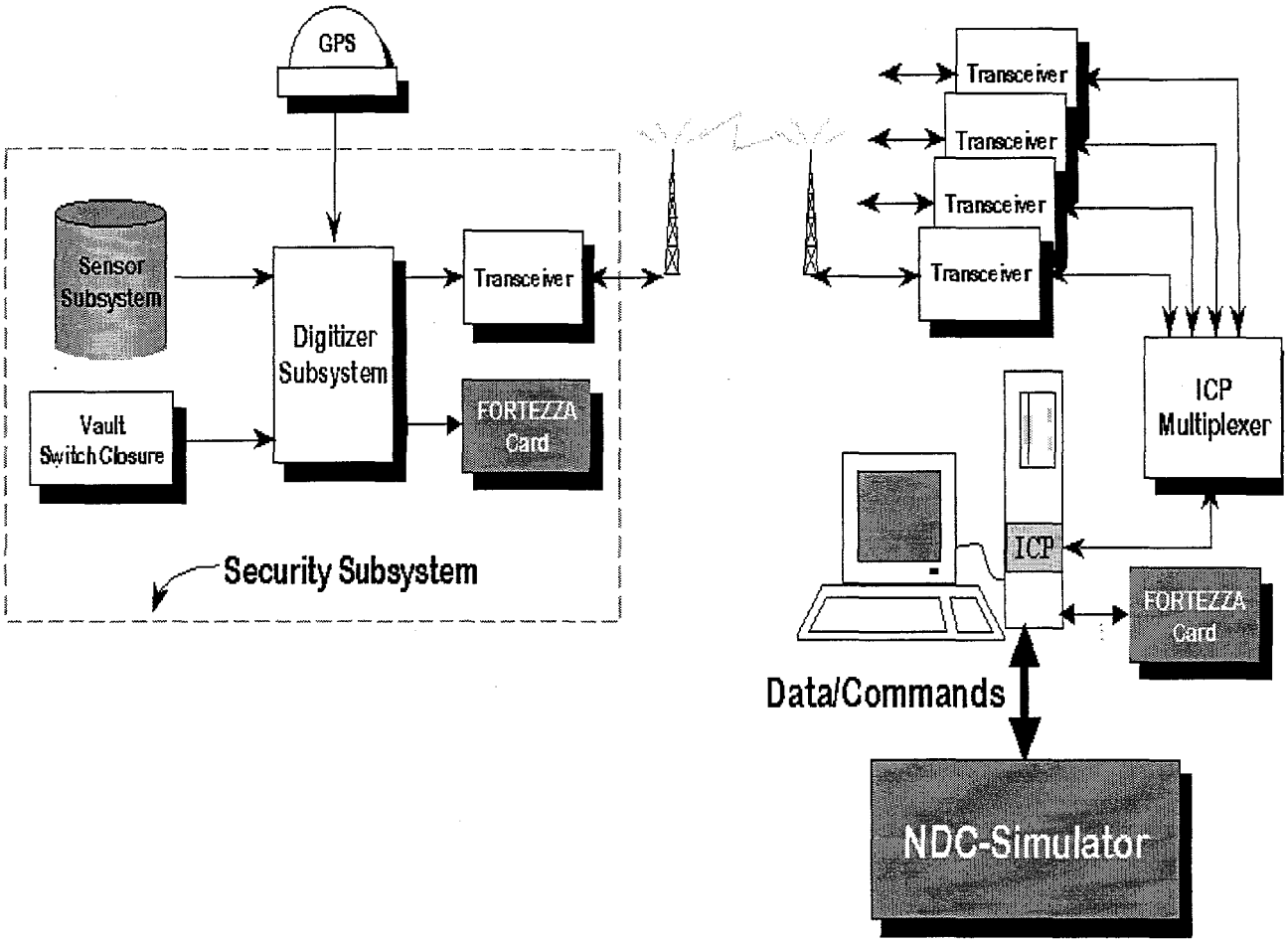

Figure 4. Diagram of DOE Prototype Infrasound Station.

process where data are available in digital form." A demonstration of authentication equipment was conducted at the DOE Prototype Infrasound IMS Station at Los Alamos, NM, during September, 1998 (Figure 4). This demonstration illustrated the feasibility of hardware authentication for sensor data and commands in a new system.

Los Alamos Demonstration

We demonstrated a cost-effective solution to signing all data channels at the remote digitizers located with the sensors of the DOE Prototype Infrasound Array. Commercial off-the-shelf hardware was used (FORTEZZA PC card). The FORTEZZA PC card and software libraries (e.g. CI Library, CM Library, card reader drivers, Alpha Protocol libraries) were used to the extent possible. Also, a command authentication system using the proposed command message format [3] was demonstrated. An NDC-Simulator (Sun SPARCstation with a FORTEZZA card) was used to verify the authenticity of the infrasound data and to generate signed commands. The activities during this demonstration were identical to those during the Pinedale demonstration with the exception that data were signed at the digitizers at the individual sensors rather than at the communication hub.

Demonstration of key management for sensor data and command authentication.

Concepts for the underlying key management system that allows one to trust the keys used in data and command authentication have been developed and demonstrated by Sandia National Laboratories. This key management

infrastructure involves the use of distributed trust models that are crucial to the international CTBT monitoring environment.

An initial demonstration of the key management concept based on distributed trust was conducted at the "Informal Workshop on Authentication and Communications" in Paris during early July, 1997. Equipment was provided by CERTCO to demonstrate activities necessary for a certification authority based on distributed trust. This demonstration involved registering a public key with the IDC's signing officers, signing of a public key certificate using threshold cryptography, and storage of the certificate in a certificate database.

The next demonstration showed as completely as possible all the key management activities throughout the life of a key in the IMS/IDC. These activities included the following.

IDC Private/Public Key Pair Generation and Public Key Distribution

All participants in the CTBT interested in verifying certificates will meet with the members of the IDC to witness the generation and release of the IDC's public key. The private key of the IDC should, of course, never be known to anyone. The best way to maintain secrecy of the IDC's private key is to distribute the private key among many parties who are not likely to collude [4]. Acting as the Certification Authority of sensor public keys (the root of trust in the keys), it is appropriate for the IDC to distribute its public key in a face-to-face meeting. This meeting is the bootstrap step of the entire key management process. Other public key exchanges can occur at this meeting as well. For example, the Observer will generate a private/public key pair and distribute its public key to the IDC and to monitoring stations. The NDC may have a public key to distribute to enable authenticated communications.

On-site Sensor Private/Public Key Pair Generation

The sensor key generation process is critical to trusting the signatures produced by the sensor's authentication unit. Upon startup, the authentication unit will utilize a default private key, but allow the issuance of a command to generate a new private key. At each sensor site, Observers, acting on behalf of the PTS, will issue a key generation command to the sensor's authentication unit, acquire its public key, and send it to the IDC as part of a signed request to certify. After a new key has been generated, only a key update command from the IDC should be allowed.

Sensor Public Key Certification

Upon receipt of an Observer's request to certify a sensor system's public key, the IDC will create a certificate for the key and electronically distributes the certificate to interested NDCs (signed with the IDC's private key) and/or place it in a certificate directory for later access.

Sensor Public Key Certificate Distribution and Verification

Recipients of IMS sensor data require the unique public key associated with that sensor in order to verify the authenticity of the data. Having the IDC's public key, NDCs can verify the authenticity of certificates and utilize the certified public keys for sensor data verification.

Sensor Private and Public Key Usage

The sensor system will sign sensor data and communicate it to the NDC/IDC. Following verification of the sensor's certificate using the IDC's public key, the sensor's public key will be extracted from its certificate and used to verify sensor data signatures.

Remote Sensor Key Updates

The IDC will remotely issue a signed key update command to an IMS sensor and receive, certify, and distribute the new public key generated by the sensor's authentication unit. In detail, the sensor will 1) verify the signed key update command using the IDC's public key, 2) generate a new private/public key pair, 3) sign the new public key with the old private key, and 4) begin using the new private key for sensor data authentication. If the sensor system's private key is trustworthy, then the newly generated public key communicated by the sensor system can be trusted as well. When the IDC receives the signed public key from the sensor system, it creates a new certificate for that system and distributes it in the usual way.

Figure 5 illustrates the IMS key management demonstration. The demonstration involves four computers representing the monitoring or sensor system, the IDC, an NDC, and an on-site observer acting on behalf of the certification authority. The various steps involved in the key management process as described above are depicted with data flows and their associated order in time indicated with the numbered circles.

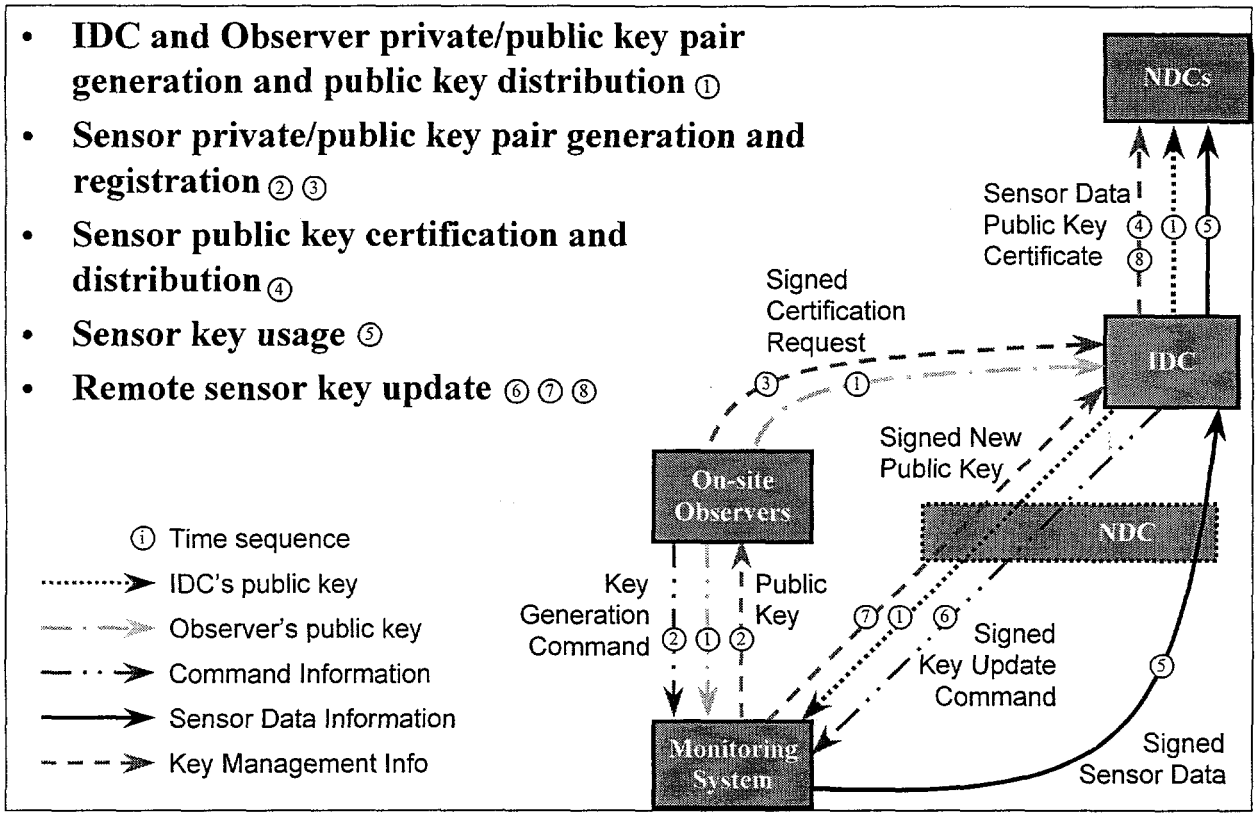

Figure 5. Key Management Demonstration Block Diagram.

CONCLUSIONS AND RECOMMENDATIONS

The Station Authenticator used in the Pinedale demonstration is applicable to existing IMS stations that transmit Alpha protocol data from the station. Using the demonstrated hardware, estimated cost of retrofitting an existing IMS station is $5000 with two weeks integration, testing, and installation effort per station. Note that the demonstrated hardware (Sun SPARCstation 5) is no longer available from Sun Microsystems, though it should be available from other sources. The Sun Ultra 5 workstation should make an acceptable replacement at the same cost with some additional development effort. It may also be possible to run the demonstrated software on existing station equipment. The signature verification programs used on the NDC Simulator may also be used at the NDC.

The costs of including data authentication at the digitizers of the various sensors will be available in October, 1998. Non-recurring engineering costs experienced by other vendors who provide this instrumentation should be similar to those required for the Los Alamos demonstration.

The tasks involved in each step of key management are neither difficult nor time-consuming to conduct. . Much of the effort occurs during the initialization phase and will not be repeated.
The training for personnel required to perform PTS Observer tasks will be typical use of laptop computers.
The key management system will likely require a system administrator or this function which could be shared with other elements of the IDC.

REFERENCES

1. *Task Leader Guidelines on Authentication,* CTBT/PC/III/WGB/TL/52/Rev1, 14 August 1997.
2. *Task Leader Guidelines on Authentication,* CTBT/PC/V/WGB/TL/92, 21 January 1998.
3. *The PTS Response to Technical Issues on Authentication,* CTBT/WGB-6/PTS/CRP.33, 3 June 98.
4. P. Herrington, T. Draelos, R. Craft, E. Brickell, Y. Frankel, and Mark Silvestri, "A Key Management Concept for the CTBT International Monitoring System", *19th Seismic Research Symposium on Monitoring a CTBT,* December September, 1997.