Paper Number: IAEA-CN-220-204

Key Management Strategies for Safeguards Authentication and Encryption[1]

Michael Coram,[2] Ross Hymel, Michael McDaniel, and Jay Brotz

Sandia National Laboratories[3]
P.O. Box 5800
Albuquerque, New Mexico 87185-1374
United States of America

Abstract. For remotely transmitting monitoring devices used within international safeguards, there is the need to ensure monitoring data from that device is accurate, authentic, and confidential. If an adversary can modify messages, insert fake messages, or even view messages, the Inspectorate's ability to validate Operator declarations may be compromised. Encryption and digital signatures support the required accuracy, authenticity, and confidentiality of the data but challenges exist in managing the cryptographic keys they require. The keys must be protected to ensure they are not stolen or forged. Additionally, the keys must be tracked and associated with the device that uses them to ensure that decryption and signature validation can occur. Four generations of remotely transmitting monitoring devices have been developed by Sandia National Laboratories, with each improving on the key management capabilities of the previous generation. This paper will explore those generations, showing how the strategies they utilize can help make key management easier.

1. Introduction

Cryptography is essential for ensuring data from remotely transmitting devices is accurate, authenticate, and confidential. It prevents an adversary from modifying legitimate data (accuracy), injecting forged data (authenticity), and viewing data (confidentiality). However, cryptography requires the use of keys, which must be managed. Key management includes ensuring an authentic key is obtained from the remotely transmitting device, protecting that key against theft or forgery by an adversary, and associating specific keys with the device that uses them. Key management can become more difficult as the numbers of keys increase just because of the number of keys that need to be managed.

To place key management in context, a simple monitoring scenario in which the use of cryptography can be explored is provided. *Figure 1* provides a simple illustration of this scenario. In this scenario, a country has agreed to place material under international safeguards at an Operator facility. An Inspectorate places a set of item monitors on the containers that store this material. Sandia National Laboratories (SNL) has developed the Remotely Monitored Sealing Array (RMSA), a remotely transmitting item monitor that will be discussed in this document. The RMSA is a battery powered item monitor that contains a fiber optic loop seal. If the container is opened, the seal is broken and a message is sent to the Inspectorate. Since the container and its item monitor reside at an Operator facility, the message naturally travels through that facility on its way to a data management system residing at the Inspectorate's headquarters. While the requisite networking equipment may be provided and controlled by the Inspectorate, it still resides at the Operator facility where it could be at risk of intrusion by an adversary. In this context, the Operator is considered an adversary. The Inspectorate does not trust the Operator and thus needs to ensure that the data received is authentic, accurate, and confidential. In this scenario, it is assumed that the monitoring data is not provided to the Operator. Once the data leaves the Operator facility, it is assumed to travel over the Internet, as a cost effective solution to long distance data transfer. Additional adversaries exist on the Internet and the requirements for authenticity, accuracy, and confidentiality are just as necessary.

---

[1] SAND No. 2014-XXXX
[2] Corresponding author, mcoram@sandia.gov
[3] Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

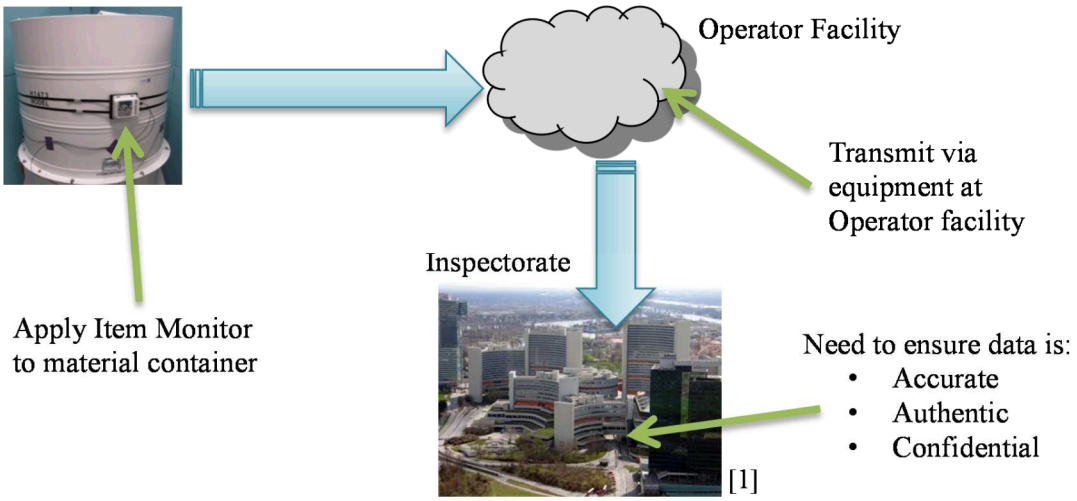

Figure 1. Simple Monitoring Scenario

To ensure accuracy, authenticity, and confidentiality, the item monitor digitally signs and encrypts all messages that it sends. A digital signature is unique to a given item monitor and message. Thus, it provides both accuracy and authenticity. If a message is modified while in flight or an entire message is forged, the digital signature will not be verified. Encryption also ensures accuracy since an attempt to modify an encrypted message will result in a malformed message after decryption that can be easily detected by the Inspectorate. Encryption also provides confidentiality as only the holder the appropriate decryption key can decrypt the message.

Both digital signatures and encryption occur at the source (within the item monitor) to reduce the opportunity for an adversary to tamper with the message. In addition, the item monitor can detect an attempt to gain access to its internals. If such a tamper attempt is detected, the item monitor destroys its cryptographic keys and reverts to a default key. The Inspectorate can detect the use of this default key and determine that tampering may have occurred with the device.

There can be a large number of item monitors at a single facility, and even more on a global scale. This presents a problem for key management just because of the potential number of keys to be managed. The remainder of this paper discusses how key management can be simplified by presenting four generations of an SNL Item Monitor, starting with the RMSA as Generation 1. Each generation builds on the previous to simplify key management.

It should be noted that, while this paper focuses on an item monitor for simplicity, other SNL-developed monitoring technologies have the same capabilities. In addition to the SNL Item Monitor, an authenticated camera, motion detector, and door switch have been developed. All of these monitoring technologies will leverage the key management strategies discussed in this paper, with the goal of having all technologies supporting Generation 4 by the end of 2016.

2. Generation 1 – Symmetric Key Cryptography

The first generation of the SNL Item Monitor is the RMSA. The RMSA uses symmetric key cryptography is used for both digital signatures and encryption. In symmetric key cryptography, a single key is shared between the item monitor and the Inspectorate's data management system that receives its data. This shared secret is used by both sides to perform the cryptographic operations. As a simple example, consider ***Error! Reference source not found.*** below.

The same key is provided to both the Sender (the item monitor) and the Receiver (the Inspectorate's data management system). In the case of the RMSA, the key is manually loaded upon its initialization and separately manually uploaded to the data management system. This key is then used to perform the appropriate cryptographic functions.

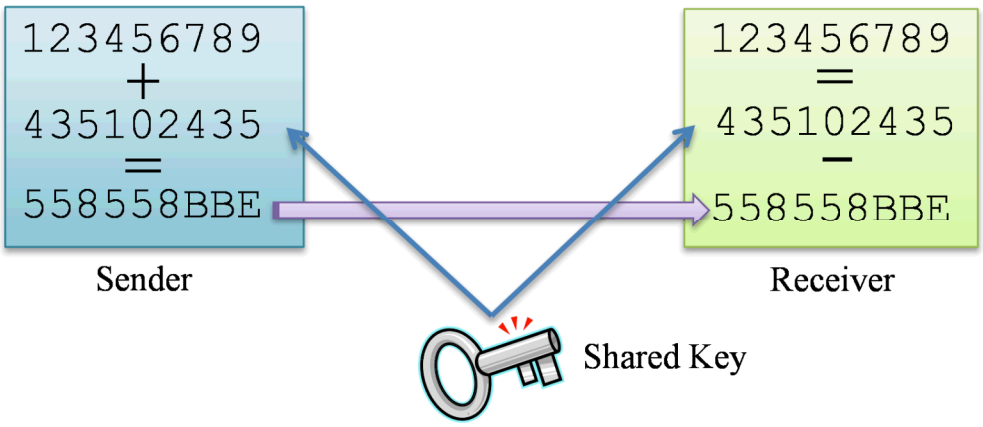

Figure 2. Symmetric Key Cryptography

The weakness with symmetric key cryptography is that anyone who has a key can perform encryption or generate digital signatures using it. If an adversary obtains both the digital signature key and the encryption key, he could forge messages from an item monitor that the Inspectorate would think is authentic. This is a significant weakness in symmetric key cryptography, and especially in the Generation 1 implementation. Since the keys are loaded during initialization, they exist externally to the item monitor where they are susceptible to theft by an adversary. This problem is exacerbated by every item monitor having two unique keys – one for encryption and one for digital signatures. If there are a large number of item monitors, there are a corresponding large number of keys to manage. These keys must all be tracked, loaded onto the correct devices, and appropriately protected.

With these weaknesses in symmetric key cryptography, one might question why it would be used. Symmetric key cryptography has a significant advantage in computational complexity. Alternatives (most prominently asymmetric key cryptography described below) can be much more computationally intensive [2]. For a device like the RMSA, which is battery powered with an expected lifetime of several years, computational power matters significantly. Using symmetric key cryptography allows for appropriate security while still allowing for significant battery life. It also allows for the use of more simple electronics, which are cheaper and potentially easier to inspect physically for hidden features. If an Inspectorate does not trust the item monitor's designer or manufacturer, they could examine the hardware and even perform destructive analysis to ensure that it is built to its design. Simpler components are easier to inspect in this way.

3. Generation 2 – Asymmetric Digital Signatures

Advances in computer processing capabilities have opened up alternatives to symmetric key cryptography. The main alternative is asymmetric cryptography. Asymmetric cryptography uses a pair of keys – a public key that can be readily shared and a private key that is not shared. Data encrypted by the private key can only be decrypted by the public key. The reverse is also true – data encrypted by the public key can only be decrypted by the private key. ***Error! Reference source not found.*** shows a simple asymmetric encryption example. The sender encrypts the data using its private key and sends over the resulting cipher text. The receiver uses the sender's public key to decrypt the cipher text.

Since anyone with the public key can decrypt the data and the public key can be widely shared, it clearly is not useful for confidentiality. By reversing the process in **Error! Reference source not found.**, asymmetric cryptography can be used to ensure confidentiality. If data is encrypted using a public key, only the holder of the private key can decrypt it. If the item monitor were to have the public key of the data management system, it could use asymmetric cryptography for encryption. However, there is a significant downside. Asymmetric cryptography is significantly slower than symmetric cryptography [2]. Additionally, the performance of asymmetric cryptography is directly correlated to the size of the data being encrypted [3].

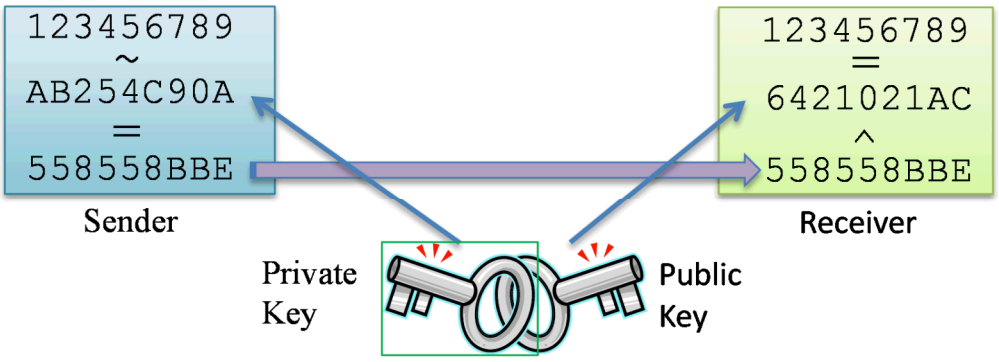

Figure 3. Asymmetric Key Cryptography

Since messages can be quite large, using asymmetric cryptography for encryption was considered impractical for the RMSA. Instead, Generation 2 of the SNL Item Monitor only uses it for digital signatures. All generations of the SNL Item Monitor utilize symmetric cryptography for encryption for power consumptions reasons.

With asymmetric digital signatures, the sender generates a hash of the message it wishes to sign, encrypts that hash, and provides it to the receiver with the message. Since the hash of a message is usually substantially smaller than the message itself, encrypting the hash is less costly than encrypting the entire message. The receiver generates the same hash of the message, decrypts the hash generated by the sender, and compares them. If an adversary attempted to modify the data in flight or insert a forged message, the hashes will not match. The adversary does not have the sender's private key, so cannot create a valid signature.

The strength of asymmetric cryptography is that it is considered extremely difficult to determine the private key given only the public key – as in, it would take decades for even the most power computing platforms given a reasonable key size [4]. This has two advantages for key management. First, it means that the theft of a public key by an adversary has less of an impact. The adversary can only verify signatures, which would not affect the accuracy, authenticity, or confidentiality of messages sent from the item monitor to the Inspectorate. Second, the key pair can be generated by the item monitor itself, rather than requiring it to be loaded during initialization. This means the private key can be generated and kept internally on the item monitor. If the private key were obtained, an adversary could easily forge signatures and modify messages or interject fake ones, but the device can appropriately protect it. It can destroy the private key should the item monitor detect any attempt by an adversary to gain access to its internal components. The SNL Item Monitor implements this protection.

However, an adversary has a second avenue of attack. Generation 2 suffers from a vulnerability known as a man-in-the-middle attack. This weakness exists because of how the public key is obtained from the item monitor. The current implementation provides the public key as part of an association message sent when the item monitor first connects to the data management system. Since the Operator controls this network, it can intercept the public key and replace it with a public key that it generates.

As shown in ***Error! Reference source not found.***, the item monitor generates a key pair (1) and sends the public key over an untrusted network (2). It is intercepted by the adversary and replaced with the adversary's public key (3). The Inspectorate's data management system is therefore sent the adversary's public key (4) that it thinks belongs to the item monitor. Then the item monitor creates a message and signs it using its private key (5). Like the public key, this message is intercepted by the adversary (6), modified, and signed with the adversary's private key (7). The data management system gets this newly signed message (8) and verifies the signature (9).

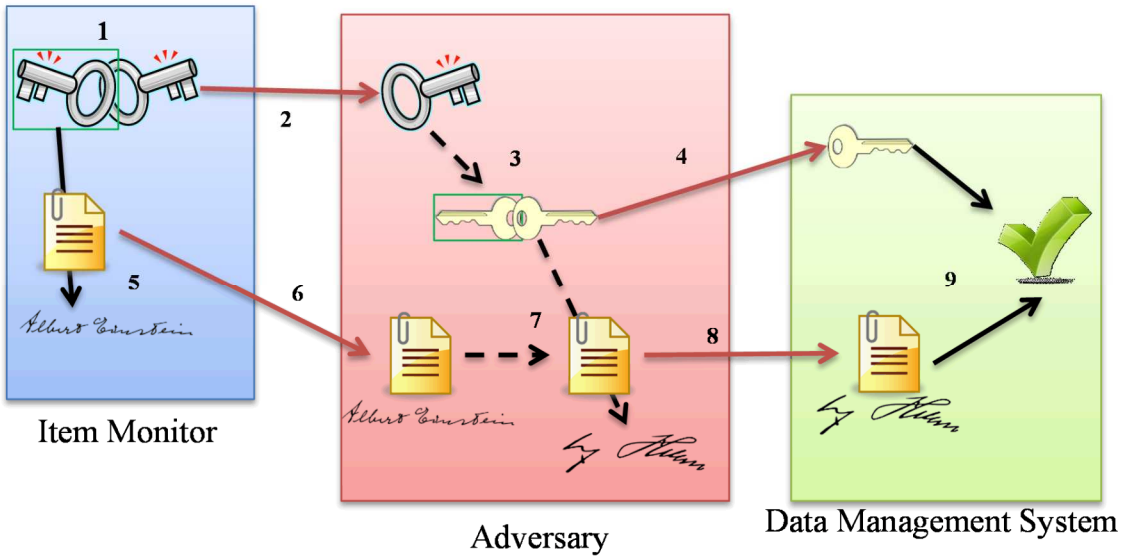

Figure 4. Man-in-the-Middle Attack

Because the signature and public key were both provided by the attacker, the signature will be verified and data management system will think the message is valid. This is the essence of a Man-in-the-Middle attack. This attack is greatly complicated by the use of encryption. Without the encryption key, an adversary cannot replace the key without detection. Since Generation 2 still uses a symmetric key loaded during initialization that is vulnerable to loss, there is still a risk.

Note that this attack could be prevented if the Inspectorate could receive the public key in a trusted manner from the item monitor. For example, it might be manually obtained directly from the item monitor during initialization in a trustable manner. However, this would require the Inspectorate to manage these public keys. There is still a key for every item monitor that must be linked to that item monitor to ensure proper validation of the digital signatures. All of the keys must be appropriately protected. In addition, this can present an operational burden as the public keys must be obtained from the item monitor and loaded into the data management system. If the keys are intercepted at any point, a man-in-the-middle attack could occur. Thus, Generation 2 has only marginally improved key management. The private key is at least protected internally in the item monitor, which is an improvement over symmetric cryptography for digital signatures, and the loss of the public key does not allow an adversary to forge a message. However, additional improvements are needed.

4. Generation 3 – Signing Authority

To address the Man-the-Middle-Attack, SNL borrowed from the concept of a Certificate Authority used on the Internet. With secure web sites, it is not necessary for a user to have the certificate for every secure site he visits to trust that he is browsing to that site. Instead, when a user browses to a site, he is presented with a certificate that is signed by a Certificate Authority. If he trusts that Certificate Authority, then the site's certificate can be trusted. This approach has been modified for use with the SNL Item Monitor as part of Generation 3. Generation 3 relies on a new Signing Authority akin to the Internet's Certificate Authority. The use of a certificate, which holds details such as validity dates, valid uses for the key, and an elaborate "Common Name," [5] was not deemed useful in this context, though it would be possible to support it.

The Signing Authority is a device controlled by the Inspectorate that allows the trust of the item monitor's public key to be established without requiring the manual transfer of the key. When the item monitor is initialized, it communicates with the Signing Authority to establish the trust relationship. ***Error! Reference source not found.*** shows how the Signing Authority helps establish this trust.

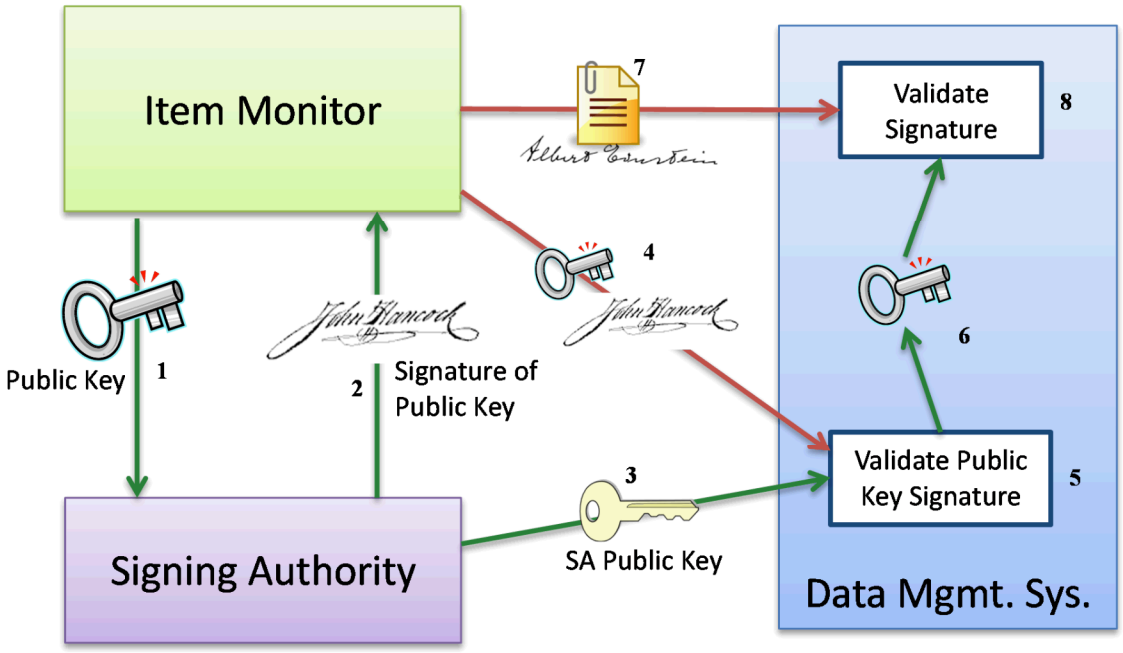

Figure 5. Signing Authority

During initialization, the item monitor generates its key pair and sends the public key through a secure channel to the Signing Authority (1). For example, the item monitor could be initialized at the Inspectorate's headquarters. This is similar to the need to load the symmetric encryption keys or obtain the public key in Generations 1 and 2 respectively. Those activities must also occur in a secure location. The Signing Authority signs the item monitor's public key and returns the signature to the item monitor (2). At any point in time, event well in advance, the Signing Authority's public key is loaded into the Inspectorate's data management system (3). Since the Inspectorate controls the Signing Authority, this can happen in a trusted manner. When the item monitor associates with the data management system, it can now provide both its public key and the Signing Authority's signature of that public key (4). This transmission occurs on a network controlled by the Operator and thus considered untrusted by the Inspectorate. The Inspectorate can validate the signature of the item monitor's public key since it has a trusted copy or the Signing Authority's public key (5). This key can then be stored (6), though it can be re-requested and revalidated at any time. The Item Monitor can now send data and sign it with its private key. Because data management system has a trusted copy of the item monitor's public key, it can validate the message signature (8).

This approach eliminates the Man-in-the-Middle vulnerability. If an adversary were to intercept the association message, which contains the item monitor's public key and that key's signature, they could not replace the public key without detection since they cannot forge the key's signature. It also aids in key management as the public key of the item monitor can be exchanged and validated after initialization. This prevents the manual step of obtaining the public key from the item monitor and loading it into the data management system. This operation can occur automatically over the network.

While the trust relationship so far is unidirectional, with the data management system establishing trust of the item monitor's public key, it can be bi-directional. The public key of the Signing Authority can be loaded onto the item monitor during its initialization. In addition, the data management system can have its own key pair. During that system's initialization, its public key can be signed by the Signing Authority. When an item monitor associated, the data management system can now provide the item monitor with its public key and the Signing Authority's signature of that key. This allows the item monitor to trust that it is communicating with an authentic data management system, in a mirror of the process described above.

This trust relationship is critical for an item monitor if it receives messages from the data management system. The SNL Item Monitor can receive a set of commands from the data management system, so this trust relationship allows it to ensure those commands are authentic and accurate. Generation 3 supports the establishment of a bi-directional trust relationship between the item monitor and the data management system. This relationship is critical for Generation 4.

5. Generation 4 – Dynamic Encryption Keys

In all three generations discussed above, encryption is performed using symmetric keys that are generated externally and loaded during initialization. While encryption can be performed using asymmetric keys, it requires substantial computational power as discussed previously. However, the SNL Item Monitor's symmetric encryption implementation presents a key management concern since each item monitor utilizes a unique encryption key, requiring each key to be tracked, associated with the specific item monitor that uses it, and protected against theft by an adversary. All item monitors could utilize the same key, but this means that the compromise of this single key compromises the encryption of all item monitors.

An alternative is for the encryption keys to be generated dynamically rather than loaded during initialization. Both the item monitor and the Inspectorate's data management system can dynamically generate a portion of the symmetric key, which is exchanged with the other side. The bi-directional trust relationship between the item monitor and the data management system, established via the Signing Authority, can be used to ensure secure exchange. This key exchange is shown in *Figure 6*. Focusing on the exchange between the item monitor and the data management system, the process starts by the item monitor generating a new, ephemeral key pair (1) that is used only for this key exchange. Once the exchange has been completed, the ephemeral key pair is discarded. While the permanent key pair could be used this key exchange, the use of ephemeral keys protects against the future loss of the permanent private key. An adversary could record all of the data and then obtain the item monitor's private key from inside the device. While the permanent private key might be obtained in this way, the ephemeral private key cannot. As a result, the encryption key, and therefore communication, is still secure. This is known as Perfect Forward Security (PFS) [6]. The item monitor's tamper detection capabilities protect against the loss of the permanent private key, but an adversary's capabilities are always improving. PFS thus protects against future threats.

Continuing with the dynamic key exchange, after generating the new, ephemeral key pair (1), the item monitor signs the public key of this new key pair with its permanent private key (2). The item monitor then sends the ephemeral public key and its signature to the data management system (3). The data management system validates the signature using the item monitor's permanent public key (4).

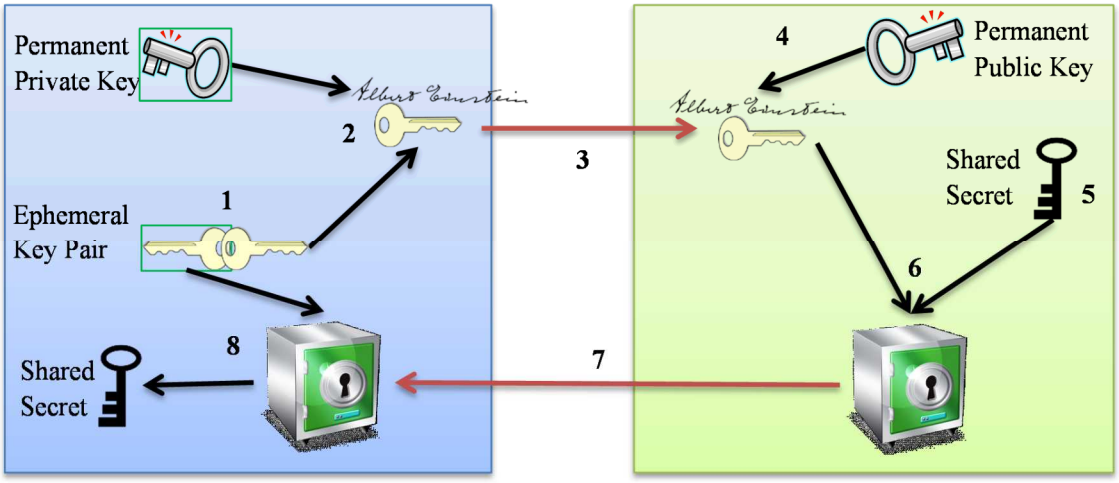

Figure 6. Dynamic Key Exchange

Because the permanent public key is already trusted thanks to the Signing Authority, the ephemeral public key can be trusted. The data management system then generates half of the shared secret key (5) and uses the ephemeral public key to encrypt it (6). One advantage of asymmetric key cryptography is that the public key can be used to encrypt data that can only be decrypted by the private key. The encrypted shared secret is sent to the item monitor (7), which uses the ephemeral private key to decrypt it. The ephemeral keys can now be thrown away to ensure PFS. This process is repeated in the reverse direction, with the data management system generating an ephemeral key pair and the item monitor using it to exchange the other half of the encryption key securely.

By dynamically exchanging the encryption key, Generation 4 eliminates the manual step of loading the symmetric encryption key during initialization, reducing the key management burden of the Inspectorate. In addition, the encryption key can be renegotiated at any time by simply repeating the process described above. This can be done periodically so the same key is not used for the lifetime of the device. Additionally, renegotiation may be useful in a joint use scenario where monitoring data is shared with the Operator, but only after the Inspectorate has confirmed its declarations. The encryption key can be renegotiated and then the previous key provided to the Operator along with the encrypted data. The Operator can decrypt that data, but cannot decrypt the current data stream. Additionally, the item monitor's public key can be shared, allowing the Operator to validate the authenticity of the messages. Because that public key can only verify signatures, there is little risk in sharing it.

6. Conclusion

By Generation 4, the SNL Item Monitor, along with other monitoring technologies developed by SNL, will support accurate, authentic, and confidential communications of monitoring data with simplified key management. The Inspectorate will not need to manually load, track, and protect the large number of keys used for digital signatures and encryption. Only a single key pair, the Signing Authority's key pair, will need to be closely protected. Keys can be dynamically exchanged over an untrusted network without compromising security, reducing the key management burden.

7. References

[1] "IAEA Vienna" by Sarajevo-x at en.wikipedia [Public domain], via Wikimedia Commons. http://commons.wikimedia.org/wiki/File:Iaea-vienna.JPG. [Accessed 20 August 2014]

[2] A.-K. A. Tamimi, "Performance Analysis of Data Encryption Algorithms," August 2006. http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/#2_4_2. [Accessed 20 August 2014].

[3] Certicom Corporation, "An Elliptic Curve Cryptography (ECC) Primer." https://www.certicom.com/images/pdfs/WP-ECCprimer.pdf. [Accessed 21 August 2014].

[4] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra and P. L. Montgomery, "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography," September 2009. http://lacal.epfl.ch/files/content/sites/lacal/files/papers/ecdl2.pdf. [Accessed 20 August 2014].

[5] R. Housely, W. Ford, W. Polk, and D. Solo, "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile," January 1999. https://www.ietf.org/rfc/rfc2459. [Accessed 9 September 2014].

[6] W. Diffie, P. C. van Oorschot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges," March 1992. http://www.scs.carleton.ca/%7Epaulv/papers/sts-final.pdf. [Accessed 9 September 2014].

[7] This work was funded by the United States National Nuclear Security Administration Office of Nuclear Safeguards and Security and Office of Defense Nuclear Nonproliferation Research and Development. Their continued support is greatly appreciated.