PKI: The DoD’s Critical Supporting Infrastructure for Information Assurance

Susan Chandler
Booz Allen Hamilton

The DoD’s Public Key Infrastructure (PKI) provides general-purpose PKI services to a broad range of applications through effective use of public key cryptography. This article presents a quick overview of the Defense-in-Depth strategy, briefly explains key PKI elements and security mechanisms, and addresses how the Air Force is employing this technology to improve information assurance (IA).

As the Internet rapidly expanded in the 90s, so did the DoD’s usage of the Web to provide global support to the warfighter. The Internet, being an open environment, was not secure enough to conduct mission-critical, unclassified transactions. Therefore, to fully benefit from this new medium, a more secure capability had to be put into place. Specifically, Internet-based transactions would need to provide a reliable means to: conduct private communications between parties on the public Internet, verify a party’s identity over the Internet, replace handwritten signatures, and ensure that data is not altered during transmission.

Today, adversaries, in their current quest to subvert DoD capabilities by degrading critical information assets, are coming from all directions. Terrorists, hackers, unfriendly nation states, and various types of criminal elements—motivated by the acquisition of top-secret intelligence, financial gain, intellectual property theft, denial of service, or simply pride in exploiting a notable target—are routinely attacking DoD networks. Their methods range from passively monitoring communications to social engineering to full-blown active network attacks with viruses and other malicious means.

Consequently IA, at least in DoD terms, is achieved when information and information systems are protected against such attacks through the application of critical security services such as availability, integrity, authentication, confidentiality, and non-repudiation.

Defense-in-Depth Strategy: A Quick Overview

The DoD’s Defense-in-Depth strategy is a practical method for achieving IA in today’s highly networked environments [1]. It uses a best practices approach that relies on intelligent applications of existing techniques and technologies. The strategy recommends a balance between the protection capability and the cost, performance, and operational considerations of the overall DoD mission. Comprised of a robust and integrated set of IA measures, the strategy hinges on the balanced focus of three primary elements: people, technology, and operations (see Figure 1).

The people element encompasses establishing, applying, and enforcing applicable policies and procedures, assigning roles and responsibilities, committing resources, training critical personnel (e.g., users and system administrators), and requiring personal accountability [1]. This includes establishing physical security and personnel security measures to control and monitor access to facilities and critical elements of the IT environment such as networks and systems.

A wide range of technologies are available that provide IA services and intrusion detection. To ensure the right technologies are procured and deployed, the technology element focuses on the establishment of effective policies and processes for technology acquisition and is grounded on two primary IA principles: defense in multiple places and having layered defenses.

Given that adversaries can attack from multiple points using either insiders or outsiders, protection mechanisms at multiple locations are in place to facilitate resistance to all classes of attacks [1]. Focus areas (shown in Figure 2) include defending:

- **Networks and Infrastructure.** Protecting the local and wide area communications networks and providing confidentiality and integrity protection for data transmitted over these networks.
- **Enclave Boundaries.** Deploying firewalls and intrusion detection to resist active attacks.
- **The Computing Environment.** Providing access controls on hosts and servers to resist insider, close-in, and distribution attacks.

The best available IA products can still have inherent weaknesses; therefore, multiple and layered defense mechanisms are deployed as unique barriers between the adversary and its target to deter exploitation of possible vulnerabilities, increase the probability of detection, and reduce the chances of successful penetration [1]. Focus areas include multiple supporting infrastructures:

- Deployment of nested firewalls at outer and inner network boundaries.
- Specification of security robustness of each IA component as a function of the value of what it’s protecting.
- Deployment of robust key management infrastructures and PKIs that support all IA technologies and are highly resistant to attack.
- Deployment of methods to detect intrusions, analyze and correlate the results, and then react accordingly.

PKI as a Supporting Infrastructure

Now that the big picture is in place, it’s time to illustrate how the PKI and its foundational element of public key cryptography is

---

Figure 1: Defense-in-Depth Strategy
PKI: The DoD’s Critical Supporting Infrastructure for Information Assurance

Figure 2: Defense-in-Depth Focus Areas

Figure 3: Secret Key Cryptography

PKI: The DoD’s Critical Supporting Infrastructure for Information Assurance

November/December 2009

a critical supporting infrastructure to the overall strategy. In its essence, public key cryptography provides three functions that help meet the needs of the Defense-in-Depth strategy: identity authentication, digital signatures, and public key encryption—all operating within a chain of trust.

Identity authentication establishes the validity of an entity’s claimed identity and is used in making access-control decisions. The entity may be a user, a Web service, or a device.

A digital signature is an electronic code that can be attached to data. It identifies the signer of the data and associates the signer with the data being signed. Digital signatures verify that the signer is really the person or entity he or she claims to be, or be a part of, and that the signed data was not modified.

Public key encryption allows multiple users to efficiently exchange encrypted data. Public key encryption establishes a common encryption key over the network without giving away enough information for someone observing the transaction to deduce the key. Together, digital signatures and public key encryption allow two or more communicating parties to positively identify one another and keep their communications confidential.

Public key systems issue a pair of keys to each user: a private key, which the user does not disclose to anyone, and a public key, which is publicly advertised. A signer encrypts data using the recipient’s public key, and the receiver decrypts it with their private key. Public keys are contained in data structures called certificates. Certificates contain a digital signature from an issuing authority and the user’s identification, which binds the user’s identity to their public key.

Several support services are required to use public key cryptography, including a means of issuing, distributing, and advertising keys and certificates; a way to verify certificate authenticity; and a process to revoke them. These services are provided by an integrated combination of equipment and administrators collectively known as the PKI.

One more component is required to implement public key cryptography: computer applications that support its use. The PKI provides a credential service for these applications. Applications are not directly part of the PKI, but public key-enabled applications improve access control by leveraging PKI-based identity authentication, and digital signatures on electronic forms automate many business processes that traditionally rely on the exchange of paper forms and handwritten signatures. Public key encryption provides confidentiality for sensitive, unclassified data over the non-secure IP Router Network (NIPRNet) and

...
providing confidentiality through encryption, public key cryptography is used for digital signatures' and identity authentication.

**PKI Core Services**

As the DoD becomes increasingly reliant on computer networking to achieve information superiority over adversaries, the core services provided by a PKI (i.e., authentication, integrity, confidentiality, and non-repudiation) become increasingly critical.

**Identification and Authentication**

Identification is defined as the process an information system uses to recognize an entity, while authentication is a security measure designed to establish the proper assurance level of a claimed identity [2]. A user's identity is authenticated as part of the certificate-issuance process. Identification and authentication are useful for granting authorization to information on a server via remote access, protecting network management from masqueraders (i.e., persons attempting to use counterfeit or stolen credentials and gaining physical access to a restricted area).

**Data Integrity**

Integrity is the assurance of non-alteration and it is this security service's job to detect unauthorized modification or destruction of information [2]. Digital signatures support data integrity verification. In contrast to handwritten signatures, verification of a digital signature relies on the authentication of the signer's identity and proves that the data remains unchanged.

**Non-repudiation**

Non-repudiation provides undeniable proof of a party's participation in a communication. The basic idea is that a user is cryptographically bound to a specific transaction in such a way that they cannot deny (repudiate) having conducted the transaction [2]. Activities such as command and control, official release of procurement documents, and travel reimbursement approvals are accompanied by legal requirements for non-repudiation. The DoD satisfies these legal requirements with PKI's digital signature capability.

**Confidentiality**

Confidentiality is the assurance of data privacy. It ensures that information is not disclosed to unauthorized persons, processes, or devices [2]. Various types of transactions—such as Web-based access, file transfers, network management, payment transactions, and secure messaging—require confidentiality to protect sensitive unclassified message data against eavesdropping, that is, unauthorized persons or entities being able to gather information byactively or passively monitoring network traffic [3, 4, 5, 6].

**Multiple Assurance Levels: Not All Information Is Created Equal**

As a credential service, a PKI binds user and entity identities with digital certificates and associated public keys. The level of assurance of a public key certificate is an assertion by a Certification Authority of the degree of confidence a relying party may reasonably place in the binding of a user's public key (and thereby the private key) to the identity and privileges asserted in the certificate [7]. The processes and controls employed in PKI operations, the methods used to protect the users' private keys, and the strength of the cryptographic algorithms used, all serve a role in determining the PKI's assurance level.

Not all information is created equal... Some types of information are extremely valuable to an attacker, while others have almost no value. On the other hand, some information may be freely disclosed but would be disastrous if it was corrupted or destroyed.”

---

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Non-repudiation</th>
<th>Identification and Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality is the assurance of data privacy. It ensures that information is not disclosed to unauthorized persons, processes, or devices.</td>
<td>Integrity is the assurance of non-alteration and it is this security service's job to detect unauthorized modification or destruction of information.</td>
<td>Non-repudiation provides undeniable proof of a party's participation in a communication. The basic idea is that a user is cryptographically bound to a specific transaction in such a way that they cannot deny (repudiate) having conducted the transaction.</td>
<td>Identification is defined as the process an information system uses to recognize an entity, while authentication is a security measure designed to establish the proper assurance level of a claimed identity.</td>
</tr>
</tbody>
</table>

---

**Security Mechanisms**

**Key Exchange**

Key exchange is the process that communicating parties use to establish a common key for secure communications. There are several ways an originating party can obtain the receiving party's public key: from a directory, directly from the receiving party as part of an online key exchange protocol, or from a cache (if the originating party had some prior communication with the receiving party). Issuing Certification Authorities automatically post subscribers' public keys to the Global Directory Service, and in the Air Force, users also publish their own public keys to the Air Force Global Address List for easy access.

**Digital Signatures**

In the digital signature process (as illustrated in Figure 5), a hash algorithm (i.e., a message digest) is produced. The hash is encrypted using the signer's private key. After receiving the message, the recipient decrypts the hash using the signer's public key and compares it to a hash calculated from the received message. If the two are a match, the recipient knows that: a) the message was not changed from the time the signer applied the signature and b) the signer's private key was used; therefore, the message must have come from the signer.
Data Recovery
Data recovery is a service that enables the originator to recover inaccessible data or permits an authorized third party to gain access to encrypted information. Legitimate reasons for data recovery may be necessary: the user obtains new PKI certificates and keys, and the original key that encrypted data is no longer available; the owner departs and leaves behind encrypted official data that needs to be accessed; and for legal or intelligence investigations.

Key Escrow and Key Recovery
Key escrow is the process of storing private encryption keys for the purpose of enabling data recovery. It automatically occurs during the certificate issuance process. Digital signature keys are not escrowed.
Key recovery is the process of obtaining a copy of an escrowed encryption key and delivering it to an authorized requester. Key recovery systems store a copy of a user's private encryption key in a secured database, allowing access by authorized personnel known as Key Recovery Agents (KRAs). KRAs are highly trusted personnel responsible for recovering archived certificates in very specific situations. The process of key recovery is protected by two-person integrity; keep in mind, however, that signature keys are not recoverable.

Supporting Services
Key Generation
Key generation generates the public-private key pair that enables public key cryptography functions. User keys are encrypted onto an authorized token (i.e., a smart card) or removable storage media (e.g., a CD). The DoD ID card, known as the Common Access Card (CAC), is a smart card and is the preferred token for PKI certificates and keys [8].

Certificate Generation and Revocation
Once the key pair is generated, associated certificates are generated by the issuing Certification Authority server. For users, the process of generating keys and issuing certificates is combined.
Certificate revocation is necessary when a certificate becomes invalid before its expiration date; there's reason to believe the private key associated with the certificate is compromised (e.g., the token is lost); a user no longer represents an organization; and when information in the certificate is no longer valid. Relying parties are notified that a user's certificate is revoked via certificate revocation lists (CRLs) published by the issuing Certification Authority.

Certificate Expiration, Updating, and Re-keying
Public-private key pairs have finite lifetimes to protect against key compromise; therefore, associated certificates also include a validity period. Users must obtain new certificates in a timely fashion to prevent any disruption in service. Certificate re-key provides for replacement prior to a certificate's expiration. The process for updating or re-keying a certificate is similar to the process for initially issuing the certificate: The registration process is repeated to ensure the reason for having a certificate remains valid, and the user's identity is authenticated.

Archives
Archives provide a long-term repository for storing information. Even though the lifetime of a Certification Authority is relatively short, it may be necessary to verify signatures on old documents at a later date. To support this need, the PKI archive service stores user registration information, certificates, and CRLs issued by the Certification Authority.

Common Access Cards
First and foremost, the CAC is the official ID card for DoD members (i.e., U.S. military personnel, DoD civilians, eligible contractors, and members of foreign nations employed in support of the DoD mission).
Each CAC includes multiple storage areas, such as a bar code and an integrated circuit chip on the front of the card, and a bar code and magnetic stripe on the back. Various data elements, such as ID data, benefits information, organizational data, card management data, and PKI credentials (i.e., certificates and public/private key pair), are stored in one or more areas. Data stored on the CAC can only be accessed through secure CAC applications.
However, the CAC is much more than an ID card. Security-enhanced engineering allows the CAC to serve as the primary interface between the user and the PKI via unclassified networked devices, such as desktops, laptops, handheld wireless devices, and peripherals, enabled for PKI use.
Enabled devices equipped with a smart card reader (and configured with the appropriate middleware application, drivers, and applicable settings) facilitate improved IA on PK-enabled networks, systems, applications, and Web servers via the digital certificates and the associated public/private key.
pair embedded in the integrated circuit chip (see Figure 6).

**Public Key Cryptography in the Air Force**

In December 2005, the Air Force mission statement was revised to include cyberspace as a critical domain in which to fly and fight [9]. Emphasis in this domain includes, among other things, the defense and protection of critical communications assets. Air Force officials refer to cyberspace as the *new battlefield* where our adversaries operate and are gaining ground. According to Lt. Gen. Robert Elder, Jr., former Commander, 8th Air Force: “It’s our most vulnerable area, and because it crosses all other domains (air, land, sea, and space), it is clearly a warfighting domain” [10].

Motivated by this new focus, the Air Force has stepped up its PKI implementation initiatives and worked diligently to become compliant with DoD directives. For example, all unclassified Air Force networks and networked applications are being public key-enabled to provide more efficient IA services and stronger authentication provisions.

Throughout the Air Force, as well as in the DoD, employees use public key-enabled applications in support of their daily activities. The rest of the federal government, defense contractors and suppliers, and allies also use PKI-enabled services. Applied uses of public key cryptography in the Air Force include:

- Identification and authentication for gaining access to unclassified networked computers, restricted Web sites, applications, and other resources (instead of usernames and passwords).
- Secure client-server transactions via the Secure Sockets Layer protocol.
- Secure financial, personnel, and contractual transactions.
- Secure unclassified messaging with authentication of originator, and confidentiality and integrity of transmitted data.
- Software (code) signing to ensure the authenticity and integrity of software obtained.
- Virtual private networking via IP security.

**In Conclusion: Tangible Benefits**

Without a doubt, PKI implementation across the DoD has attracted a significant amount of attention, primarily because of its high level of security services that support the overall IA strategy. The PKI is a sound technical solution—and is not simply a neat technology lacking tangible benefits. When deployed judiciously, the PKI offers certain fundamental advantages to an organization. Its capabilities help optimize workforce productivity and improve workflow efficiencies through more automated and secure business processes—especially significant cost savings through the reduction of administrative overhead, reduction in the number of sign-on events required by end-users, and reduction in paper-based processes.

Knowing that virtually every day, every airman legitimately accessing DoD networks is using the PKI helps maintain confidence in critical electronic communications. One can take comfort in that.

**References**

5. JTF-GNO. *Public Key Infrastructure Implementation*, Phase 2, CTO 07-015. 2007.

**Notes**

1. The PKI is not simply a product, a program, or a system—nor is it software or an application. It is a complex combination of specific hardware, specialized software, tokens, established policies, and proven procedures that collectively provide the ability to authenticate identities and protect valuable information through the use of unique digital certificates and key pairs.
2. The DoD PKI Chain of Trust begins at the DoD Root Certification Authority. The Root Certification Authority’s public key certificate is signed by its own private key. It issues and digitally signs the certificates of the subordinate and intermediate Certification Authorities, who in turn digitally sign the user certificates they issue. The trustworthiness of each layer is guaranteed by the one before.
3. The key that is not publicly revealed is a *private key*, rather than a *secret key*. This avoids confusion with the secret key of symmetric cryptography if one thinks of two people sharing a secret, but a single person keeping something private [2].
4. Because of the processing expense in encrypting an entire message using public key cryptography, the digital signature process encrypts a digest of the message rather than the message itself.
5. For the purpose of this article, a *threat* is...
defined as any circumstance or event, from an authorized or unauthorized entity either inside or outside the domain perimeter, with the potential to cause harm to an information system in the form of destruction, disclosure, modification of data, and/or denial of service.

6. Encryption certificates are advertised in the DoD via the Joint Enterprise Directory Service (located at <https://jeds.gds.disa.mil>), which is the target environment, and supported by the Global Directory Service at <https://dod411.gds.disa.mil>.

7. This depiction of public key encryption and digital signatures shows text and documents as the data being protected. Public key encryption and digital signatures can be used with any type of data in a wide variety of scenarios.

8. Except for the PKI information, which is obtained from the CA, all other information about the ID card holder is obtained from the Defense Enrollment Eligibility Reporting System through the Real-time Automated Personnel Identification System. Home address and telephone number, dependent information, and medical, dental, financial, and personnel records are not stored anywhere on the CAC.

About the Authors

Susan Chandler is an associate with Booz Allen Hamilton, assigned to the Air Force PKI System Program Office at Lackland AFB, Texas. She is a 24-year veteran of the Air Force with expertise in computer operations and information systems management. She is an award-winning professional with recognized accomplishments in the areas of strategic communications and change management. Chandler has considerable experience supporting the Air Force’s transformation to a more secure environment in cyberspace operations. She has a bachelor’s degree in occupational education, an MBA, and is a Certified Corporate Trainer.

Jerrod Loyless is a senior software engineer for General Dynamics C4 Systems. He is the public key-enabling technical lead at the Air Force PKI System Program Office at Lackland AFB, Texas. Loyless served as an Air Force communications computer officer for six years before beginning work as a contractor and consultant. He has a bachelor’s degree in computer science and a master’s degree in information security, and is a Certified Information Systems Security Professional-Information Systems Security Engineering Professional, a Certified Secure Software Lifecycle Professional, and a Project Management Professional.

Software Defense Application

The DoD implemented a PKI to provide engineered solutions that now enhance the security of networked computer-based systems. Programs and applications, which carry out or support the DoD mission, require PKI services of authentication, confidentiality, technical non-repudiation, and integrity. These services are met with an array of network security components such as standardized workstation configurations, firewalls, routers, in-line network encry ptors, and trusted database servers. Public key cryptography supports and complements these component operations. As a system solution, the components share the burden of the total system security.