The DoD Public Key Infrastructure And Public Key-Enabling Frequently Asked Questions

May 3, 2004

TABLE OF CONTENTS

DOD PKI PK-ENABLING POLICY QUESTIONS 17

IMPLEMENTATION QUESTIONS 25

General PKI Questions

1. What is PKI?

A Public Key Infrastructure is the framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components of a PKI include system components such as one or more Certification Authorities and a certificate repository; documentation including a Certificate Policy document and one or more Certification Practice Statements; and trained personnel performing trusted roles to operate and maintain the system.

PKI integrates digital certificates, public-key cryptography, and Certification Authorities into a total, enterprise-wide network security architecture. A typical enterprise PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificate directories; tools for managing, renewing, and revoking certificates; and related services and support.

Back to Questions

2. What functionality is provided by a PKI?

Public key certificates provide digital signature and encryption capabilities, which can be used to implement the security services of identification and authentication, data integrity, confidentiality, and technical nonrepudiation. Note that PKI does not directly support the security services of privilege and authorization, audit, or availability.

Identification and Authentication

PKI provides identification and authentication through digital signature of a challenge. If the sender of the challenge can verify using the certificate that the challenge was signed by the holder of the private key corresponding to the public key in the certificate, then the sender knows that the entity at the other end of the transaction is the entity named in the certificate. For more information about authentication, see "How are certificates used for authentication to a web server?"

Data Integrity

PKI provides data integrity through digital signature of the information. If the recipient of digitally signed information can verify the signature on the information, then the recipient knows that the content has not changed since it was signed. For more information about digital signatures, see "What is a digital signature?"

Confidentiality

PKI provides confidentiality through encryption. If the public key in a certificate is used to encrypt information, only the entity named in the certificate can decrypt that information. PKI can be used for both encryption in transit and for encryption at rest. For more information about encryption, see "How is PKI used for encryption?"

Technical Nonrepudiation

PKI assists with technical nonrepudiation through digital signatures. If information has been digitally signed, only the entity named in the certificate had access to the private key used to sign the information, and can therefore be assumed to some level of assurance to have been the entity that generated the information. For more information about digital signatures, see "What is a digital signature?"

Back to Questions

3. What is a certificate?

A certificate, also called a digital certificate, an X.509 certificate, or a public key certificate, is a data file that binds the identity of an entity to a public key. Certificates contain the name of the entity (also called the subscriber), the validity period start and end dates, the public key, the name of the Certification Authority (CA) that issued the certificate, and an identifier that links the certificate to the Certificate Policy that describes the system under which the certificate was issued. The information contained in the certificate is digitally signed by the issuing CA and the signature is considered part of the certificate.

Back to Questions

4. What are public and private keys?

Public key technology is based on asymmetric cryptography. Unlike symmetric cryptography where the same key is used to encrypt and decrypt information, asymmetric cryptography uses two different keys. These keys are generated at the same time, and are mathematically related such that if either key is used to encrypt, the other key must be used to decrypt. The algorithms used to generate these key pairs also ensure that if one key, called the public key, is known, the other key, called the private key, cannot be easily determined.

The public key is included in certificates and is widely distributed. The private key is kept by the subscriber. Private keys used for identity and signature are never shared outside the direct control of the subscriber. Private keys used for encryption may be escrowed so that encrypted information can be recovered if necessary.

Public key technology is used for encryption, digital signature, and identity. When using public key technology for encryption, the sender uses the recipient's public key to encrypt, and the recipient must use their own private key to decrypt. When using public key technology for digital signature, the sender uses their own private key to encrypt, and the recipient verifies the signature using the sender's public key. When using public key technology for identity, the sender gives the recipient a challenge, the recipient signs the challenge using the recipient's private key, and the sender verifies the identity of the recipient by verifying the signature on the challenge using the recipient's public key and then looking at the identity information in the certificate containing the public key.

Back to Questions

5. What is a token?

NIST defines a token as “Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant’s identity.” Private keys associated with certificates are stored in tokens, which can either be software or hardware based. Software tokens for private keys are typically stored on workstations within applications. Hardware tokens are smart cards or other devices used to generate, store, and protect cryptographic information, and can themselves perform cryptographic functions.

Back to Questions

6. What is a Certification Authority (CA)

A Certification Authority (CA) is an entity trusted by one or more users to create and assign certificates. A CA that signs its own certificate is called a Root CA or a Trusted Root. CAs that have certificates issued by another CA are called Subordinate CAs. CAs are responsible for issuing certificates, publishing certificates, and revoking certificates by placing them on Certificate Revocation Lists.

Back to Questions

7. What is a subscriber?

A subscriber is the entity whose name appears as the subject in a certificate. When accepting a certificate, subscribers assert that they will use the private key associated with the public key contained in the certificate in accordance with the requirements of the Certificate Policy identified in the certificate. Subscribers can be people or systems such as web servers, firewalls, or infrastructure components.

Back to Questions

8. What is a relying party?

Relying parties are entities that use digital certificates to identify the creator of digitally signed information, verify the integrity of digitally signed information, or establish confidential communication with the holder of a certificate by relying on the validity of the binding of the subscriber’s name to the public key contained in the certificate. Relying parties may themselves also be subscribers. For example, if a person sends a signed and encrypted e-mail message, that person is a subscriber using their own private key to sign the message, and also a relying party because they are relying on the certificate of the recipient to know what public key to use to encrypt the message.

Relying parties are obligated to only use certificates for the purposes for which they were issued, as described in the Certificate Policy identified in the certificate. Relying parties are also obligated to check the validity of the certificate prior to reliance by ensuring that the CA that issued the certificate is trusted, that the certificate has not expired, and that the certificate has not been revoked.

Back to Questions

9. What is a Certificate Policy (CP)?

A Certificate Policy (CP) is a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. It may be used by a relying party to help in deciding whether the binding of the public key to the identified subscriber is sufficiently trustworthy for a particular use.

CPs include the requirements for authenticating identity to the Certificate Authority in order to obtain a certificate, the requirements for securing the PKI, and how the keys are generated and stored. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business- to-business transactions for the trading of goods or services within a given price range.

Back to Questions

10. What is a Certification Practices Statement (CPS)?

A Certification Practices Statement (CPS) is a statement of the practices that a Certification Authority employs to govern issuing, managing, revoking, renewing and/or re-keying certificates in accordance with a specific Certificate Policy. The CPS establishes the proofing requirements for identifying the private key owner that must be satisfied before creating a certificate. There is a wide range of options for how robust (and resource intensive) this proof must be. The Certification Authority employs these procedures when issuing certificates, the clarification of parties' legal rights and obligations. CPSs may also be used to define the specific requirements of entities within the PKI performing other trusted roles. CPSs are generally reviewed for compliance with their associated Certificate Policy documents.

Back to Questions

11. What is a Certificate Revocation List (CRL)?

A Certificate Revocation List (CRL) is a list of certificates issued by a specific Certification Authority (CA), which have not yet expired, but which are no longer asserted to be valid by that CA. Certificates may be revoked for a number of reasons, including a change in the information contained in the certificate or a suspected compromise of the private key associated with the public key in the certificate. CRLs are published periodically as specified in the CA’s Certification Practice Statement (CPS) and are digitally signed by the CA.

Back to Questions

General PK-Enabling Questions

12. What is PK-Enabling?

Public Key-enabling (PK-Enabling) is the process of configuring systems and applications to use certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation. PK-enabling provides applications with the capability to rely on digital certificates, either in lieu of existing technologies such as usernames and passwords, or to enhance functionality such as incorporating digital signatures or creating an encrypted channel through an untrusted network.

A PK-Enabled application is able to invoke one or more of the following public key cryptography based functions: digital signature generation; digital signature verification; encryption; decryption. In addition, the PK-Enabled application itself, or the environment in which it runs, must do the following: securely manage keys, trust anchors, and certificates; use one or more of the security services supported by the PKI by accepting and processing approved certificates; and obtain relevant certificate and revocation data.

Back to Questions

13. What is the difference between PKI and PK-Enabling?

A PKI provides the capability to generate, manage, and revoke certificates that create a binding between an entity and a public key. PK-Enabling is the process of configuring information systems to use certificates and take advantage of the certificate binding between the entity and its public key. Therefore, PKI is an infrastructure service that provides a capability, and PK-Enabling is the action of incorporating the capability into information systems that require the security services that PKI supports.

Back to Questions

14. How are certificates used for authentication to a web server?

Certificate-based authentication consists of three steps: establishing an encrypted communication channel, validating the subscriber's certificate, and performing a challenge-response between the server and the client to ensure that the user is the subscriber named in the certificate. If these three steps are successful, the server can trust that the identity of the user is the same as the identity stated in the certificate and can then map that identity to authorizations.

Establishing an Encrypted Communication Channel

This step uses a protocol known as Secure Sockets Layer (SSL), or its successor, Transport Layer Security (TLS). This protocol requires that the application server send its public key certificate to the client. The client then generates the shared secret that will be used for the encrypted channel, encrypts it with the public key in the server's certificate, and sends it to the server. The server's private key is required to decrypt the shared secret, so the client and server have now exchanged a key that is used for all further communications.

Validating the Subscriber's Certificate

After an encrypted channel has been established, the client sends the subscriber's certificate to the server. The server validates that the certificate was issued by a PKI that the server trusts, that the certificate has not expired, and that the certificate has not been revoked.

Performing a Challenge-Response Between the Server and the Client

Because certificates are public, the server must now establish that the user attempting access is actually the subscriber named in the certificate. The server sends a challenge to the client. The client digitally signs the challenge using the private key associated with the public key in the certificate and return the signed challenge to the server. The server uses the subscriber's certificate to verify the signature on the challenge.

Back to Questions

15. What is a digital signature?

A digital signature is the electronic analogue of a written signature in that the digital signature can be used by a third party to determine that the entity named in the signature did sign the information. In contrast to handwritten signatures, a digital signature also indicates proves that the information has not changed since the signing.

A digital signature is created by first creating a hash of the information, encrypting the hash with the private key, and affixing the encrypted hash to the information. A copy of the signer's certificate is generally included with the signed information.

There are three steps to validating a digital signature. First, the certificate associated with the signature is verified to have been issued by a trusted CA, and not have been revoked at the time the signature was applied. Then the encrypted hash is decrypted using the public key in the certificate. Finally, a new hash is generated of the signed information, and the value of the new hash is compared to the value of the decrypted hash. If the two hash values match, then the entity named in the certificate is likely to have affixed the signature, and the information has not changed since the signing.

A hash, also called a message digest, is generated by passing the original information to a one-way hashing algorithm which produces a number based on the original information. Hashing algorithms are designed so that it is computationally infeasible to find an alternative message that would produce an identical digest or to determine a comprehensible message from the hash.

Back to Questions

16. What actions must be taken to support non-repudiation of digital signatures?

In general, there is a particular set of information that must be archived in a reliable way and be able to be retrieved at a future date to be able to prove the validity and integrity of a signed and/or encrypted piece of electronic data. This "particular set of information" includes components that are the responsibility of the infrastructure and components that are the responsibility of the relying party.

The infrastructure must archive all of the certificates it creates and all information about certificate revocation, as well as any audit information necessary to be able to prove proper operation. This set of data will prove that the CA performed its duties as assigned and will convey when certificates were created, expired and/or revoked. It is not the responsibility of the infrastructure to keep track of the data that is passed back and forth using the certificates it creates. Thus, the relying party must preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Data format changes will invalidate signature, so it may also be necessary to preserve application versions and formatting information.

A related issue to the archiving of information for non-repudiation is the issue of trusted timestamps. It is possible that a malicious originator of data could "backdate" the time of transmission to make it appear as if it took place prior to certificate expiration or to the placement of their certificate on a CRL. To avoid this, some information systems may require a greater degree in the trust of the time stamp placed on each individual transmission. Note that since this is a per-transmission action that must be enforced by the application, it is not the responsibility of the PKI to provide this timestamp. Usually, a separate trusted time stamping service is used for this activity.

Archive sites are required to maintain either sufficient technical information to revalidate a signature (including a copy of the application necessary to validate the signature) or sufficient evidence that the signature was verified at the time of receipt.

Back to Questions

17. How is PKI used for encryption?

Public key technology is based on asymmetric cryptography. However, performing cryptographic functions using asymmetric cryptography is computationally intensive and there are limitations on the size of the information to be encrypted. Therefore, when using PKI to encrypt, a symmetric key is first generated, the information is encrypted with the symmetric key, and then the symmetric key is encrypted using the public key of the intended recipient and the encrypted symmetric key is affixed to the encrypted information. If there are multiple recipients of the encrypted information, multiple copies of the symmetric key are affixed, with each copy encrypted using a different public key.

Back to Questions

18. How do users benefit from PK-Enabling of information systems?

As more systems move towards integrating PKI capabilities, users will see significant benefits in addition to increased information assurance.

Reduced sign on

Certificate-based authentication uses the ability of the user to digitally sign a challenge using the private key associated with the certificate, instead of requiring the user to authenticate with a userid and password that are specific to the application. As a result, the user only needs to remember the PIN or password that unlocks the private key to access any PK-Enabled information system the user is authorized to access.

Portability

Because of the recognition of security problems with non-PKI based systems, specifically sending userids, passwords, and Sensitive information over unsecure networks, many information systems today are restricted for access within specific domains. As information systems become PK-Enabled, some of these restrictions are no longer necessary. As a result, users may find that they are better able to access information systems from locations other then their primary workstation.

Process automation

Paper-based processes that require signatures may take advantage of PKI capabilities to become more automated, resulting in shorter cycle times and better auditing capabilities for these processes.

Encryption

Users will benefit from some of the confidentiality and integrity services provided by the PKI. For example, web servers that are PK-Enabled encrypt communications channels between the user and the web server, ensuring that Sensitive data is protected in transit between in the communicating parties. Also, any documents or data at rest that either needs to be kept confidential or protected from unauthorized changes can utilize the services by the PKI to ensure their confidentiality and integrity. For example, an e-mail containing with personal information could be encrypted ensuring that only the intended recipient would be able to see the information.

Back to Questions

19. How does the administrator/owner benefit from PK-Enabling of information systems?

The owners and administrators benefit from PK-Enabling both in the increased assurance that public key technology integration can bring, and in long term savings in account management.

Security Requirements

PK-Enabling information systems can assist in meeting policy and security requirements for the domain in which the information system operates.

Account Administration

PK-Enabling allows information systems to separate identification and authentication from authorization. While the fact that an individual holds a certificate does not necessarily provide the information system administrator with sufficient information to determine if the user should have privileges to access the information system, it can provide the knowledge that users are who they say they are. Instead of having to create a new userid and password for each new account, the administrator can map the identity contained in the certificate to authorizations. As a result, administrators do not have to provide password management services, and a secure channel is no longer required to inform the user of their new account name and password.

Process automation

Paper-based processes that require signatures may take advantage of PKI capabilities to become more automated, resulting in shorter cycle times and better auditing capabilities for these processes.

Back to Questions

DoD PKI Questions

20. What is the DoD PKI?

DoD PKI is a fundamental component of the DoD's Net-Centric vision and is essential to providing enhanced Information Assurance and Identity Management capabilities. It provides the base level of identification and authentication, integrity, non-repudiation and confidentiality for the Global Information grid. The DoD use of PKI in our Identity Management capability is recognized as the world leader in this area.

The DoD PKI is operated under the requirements of the DoD X.509 Certificate Policy. The Root Certification Authority (CA) is operated by NSA in an off-line state. This Root CA issues certificates to on-line Subordinate CAs on both the NIPRNet and the SIPRNet. Subordinate CAs issue certificates to subscribers, including both human and non-human entities such as web servers who have been authenticated by trusted individuals including Registration Authorities, Local Registration Authorities, and Verification Officers.

The DoD PKI issues certificates to both software and hardware tokens. The primary token for individuals within the DoD on the NIPRNet is the Common Access Card.

Back to Questions

21. What capabilities are provided by the DoD PKI?

Certificate Issuance

The DoD PKI issues certificates to DoD eligible users who have been authenticated by trusted individuals including Registration Authorities, Local Registration Authorities, and Verification Officers.

Certificate Revocation

The DoD PKI revokes certificates upon request from a trusted individual such as a Registration Authority. The DoD PKI notifies relying parties of certificate revocation by issuing a Certificate Revocation List (CRL) at least daily. Each subordinate CA within the DoD PKI publishes its CRL to a central repository. The DoD PKI is also investigating providing alternate methods of certificate revocation status checking.

Encryption Certificate Publication

The DoD PKI publishes certificates that are used for encryption to a repository so that entities that wish to encrypt information for the subscriber named in the certificate can download a copy of the certificate.

Encryption Key Escrow and Recovery

The DoD PKI escrows private keys associated with certificates that can be used to encrypt information. Private key associated with certificates used for signature or identification are not escrowed. The PKI provides a key recovery capability for these private keys to support recovery of data encrypted with the public key in the associated certificate. The PKI does not provide a data recovery service.

Key recovery may be requested when a subscriber loses access to their own private key through loss or expiration of the token containing that key or when a third party requires access to encrypted data because the subscriber is not available or is suspected of criminal activity.

Back to Questions

22. What is the status of the DoD PKI?

The DoD PKI has issued identity, e-mail signing and encryption certificates to 4.5 million subscribers on the NIPRNet. Additionally, it has provided device certificates for DoD private web servers and the capability to issue code-signing certificates. Limited capability exists to perform these functions on the SIPRNet. While the DoD has obtained an Initial Operating Capability (IOC) for the functions of PKI, the DoD PKI Enterprise-wide capability will continue to expand in order to enable applications to exploit the technology. DoD Components must continue to make available and/or develop the enabling technology to integrate PKI capabilities into their information systems.

Today, the DoD has issued more than 8 Million PKI Certificates to the DoD population. DoD Components have enabled more than 50% of all of their workstations to be able to use PKI Capabilities. All DoD Private Web Servers have been PK-Enabled to use PKI for confidentiality, and there are numerous commercial and Component specific applications available to provide PK-Enabled services including client certificate-based authentication.

Initial IOC was achieved in April 2004. Other capabilities will continue to be made available to ensure that the DoD PKI is a foundation for enabling Identity Management supporting Information Assurance Component of the Global Information Grid Architecture. All DoD Components are continuing their efforts to PK-Enable applications.

Back to Questions

23. What is a Registration Authority (RA)?

A Registration Authority (RA) is an official recognized by the Certificate Authority to ensure that the subscriber's appropriately present the necessary credentials for registration into the PKI. In the DoD PKI, RAs enroll devices into the PKI, revoke user certificates and authorize Local Registration Authorities to enroll individual subscribers.

Back to Questions

24. What is a Local Registration Authority (LRA)?

A Local Registration Authority (LRA) is an individual authorized by a Registration Authority to perform identity verification of human and component applicants, and to authorize issuance of certificates to human applicants.

Back to Questions

25. What is the significance of the Common Access Card (CAC) in the DoD PKI?

The Common Access Card (CAC) is the primary token for protecting private keys associated with identity, signature, and encryption certificates issued by the DoD PKI to DoD eligible users. CACs are issued by Verification Officials who are recognized as trusted agents of the DoD PKI for issuing certificates to human applicants.

Back to Questions

26. What kind of certificates does the DoD PKI issue?

The DoD PKI supports three types certificates for human subscribers, which are used for identity, encryption, and signature. On the NIPRNet, these certificates can be in software or can be issued on CAC hardware tokens. On the SIPRNet, these certificates are only issued in software.

The DoD PKI also supports component certificates. These certificates are issued to web servers and other information systems or infrastructure components to enable them to identify themselves to users or other components, and to enable establishment of encrypted communications between components or between users and components.

Finally, the DoD PKI supports code-signing certificates. These certificates are used to digitally sign executable code to ensure the authenticity and integrity of the code.

Back to Questions

27. What is the difference between identity, signature, and encryption certificates?

Identity, signature, and encryption certificates are issued with different certificate profiles to enable different uses of these certificates.

Identity certificates are the primary certificate issued to individuals. These certificates assert digital signature and nonrepudiation and are primarily used to identify the subscriber to information systems. Identity certificates do not contain e-mail addresses.

Signature certificates are used to digitally sign e-mail and other documents. These certificates assert digital signature and nonrepudiation. They contain e-mail addresses to facilitate their use in digitally signing e-mail messages. In addition, signature certificates contain specialized information to allow them to be used to authenticate to Microsoft networks.

Encryption certificates are used to encrypt information. These certificates assert encryption and do not assert digital signature or nonrepudiation. They contain e-mail addresses to facilitate their use in encrypting e-mail messages. The private keys associated with encryption certificates are escrowed.

Back to Questions

28. What is a distinguished name?

The distinguished name is the unique identifier contained in each certificate. It is based on the X.500 directory schema. Within the DoD PKI, all distinguished names start with “c=US, o=U.S. Government, ou=DoD”. All distinguished names end with a common name, which for CACs is “lastname.firstname.mi.EDI-PI”.

Although common names are unique within the DoD PKI, they are not unique across PKIs. However, the use of the X.500 schema for full distinguished names should ensure their uniqueness across PKIs.

Back to Questions

29. What is the role of the Global Directory Service in the DoD PKI?

The Global Directory Service (GDS) is the repository for the DoD PKI. Subordinate CA certificates, CRLs, and encryption certificates are posted to the GDS by the DoD PKI and can be obtained from the GDS.

Back to Questions

30. Who can get a certificate from the DoD PKI?

DoD eligible users are active duty uniformed services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD network and e-mail services.

For personnel who are not DoD military or civilian employees, eligibility is determined based on the interaction of the individual with the DoD rather than on the type of individual. These personnel include DoD support contractors, non-US nationals, and volunteers. Individuals who access DoD information systems from a remote location, such as accessing web servers, are not generally eligible for DoD PKI certificates. Individuals who have a duty station within a DoD facility and who require direct access to DoD networks are generally eligible for DoD PKI certificates.

Back to Questions

31. How do I get a DoD PKI certificate?

CACs are issued at RAPIDS terminals. To locate the nearest RAPIDS office, visit the http://www.dmdc.osd.mil/rsl/ and search by city, state, or zip code. Note that a smart card reader and middleware are required to enable a workstation to use certificates on a CAC.access the CAC PKI certificates.

Software certificates are issued by Local Registration Authorities.

Back to Questions

DoD PKI Interoperability Questions

32. Who is not eligible for a DoD PKI certificate?

DoD eligible users are active duty uniformed services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD network and e-mail services. Individuals who access DoD information systems from a remote location, such as accessing web servers, are not generally eligible for DoD PKI certificates. Individuals who conduct business with, access DoD information systems over the Internet, or exchange e-mail with DoD entities are not eligible for DoD PKI certificates unless they also work on site at DoD facilities. DoD allies and coalition partners are not eligible for DoD PKI certificates unless they work on site at DoD facilities.

Back to Questions

33. Who needs a certificate other than those eligible for DoD PKI certificates?

DoD partners are government or non-government entities that process electronic transactions with the DoD, or exchange e-mail containing DoD sensitive information. As DoD information systems become PK-Enabled, these entities will require certificates that have been approved for interoperability with the DoD to conduct transactions.

Back to Questions

34. What is the Federal Bridge?

The Federal Bridge is an infrastructure operated by the U.S. Government to provide a mechanism for creating and validating trust between distinct PKIs. To become a member of the Federal Bridge community, a PKI must go through a rigorous process to ensure that the Certificate Policy of that PKI meets all of the requirements of the Certificate Policy under which the Federal Bridge Certification Authority (FBCA) operates. Membership in the Federal Bridge is indicated by the Root CA of the PKI issuing a cross-certificate to the FBCA, and the FBCA issuing a cross-certificate to the PKI's Root CA. For additional information, see the federal bridge home page at http://www.cio.gov/fbca.

Back to Questions

35. How will the DoD participate in the Federal Bridge?

Currently, the DoD has one-way interoperability with the Federal Bridge Certification Authority (FBCA). As a result, other members of the FBCA community can extend their trust to certificates issued by the DoD PKI.

The DoD PKI is working to establish bi-directional interoperability with the FBCA. However, it is important to note that while the FBCA facilitates trust between member PKIs, it does not require it. The DoD will continue to make interoperability trust decisions for DoD relying parties based on the requirements of DoD information systems to accept certificates from external PKIs, and DoD requirements to maintain Defense in Depth objectives.

Back to Questions

36. What is the purpose of the Interim External Certificate Authority (IECA) and follow-on External Certification Authority (ECA)?

Department of Defense (DoD) policy requires that many information systems become PK-Enabled. While all individuals who sit at DoD facilities, including military and civilian employees and contractor personnel will be issued a DoD Common Access Card (CAC) containing certificates issued by the DoD Public Key Infrastructure (PKI), there are many external entities and organizations that the DoD communicates with, through access to DoD information systems and via e-mail, that will not be issued DoD PKI digital certificates. The External Certificate Authority (ECA) program is designed to provide a mechanism for these external entities and organizations to get certificates that have been approved by the DoD as meeting the required DoD assurance level for binding the identity of the named certificate holder to the public key contained in the certificate.

The ECA program is the successor to the Interim External Certificate Authority (IECA) program that has been in effect since 1999. However, unlike the IECA program, the ECA program is not restricted for use only by DoD applications. Also unlike the IECA program, the ECA program operates under its own Certificate Policy (CP). This CP defines two levels of assurance, Medium and Medium Hardware, which have been reviewed and approved by the DoD Certificate Policy Management Working Group (CPMWG) as providing equivalent protection to the DoD software and CAC hardware assurance level requirements.

For more information about the ECA program, and for information on how to obtain certificates, see http://iase.disa.mil/pki/eca

Back to Questions

37. How do contractors obtain certificates for use with DoD information systems?

Contractors who are eligible for DoD PKI certificates should obtain certificates by being issued a CAC or a software certificate, as appropriate.

Contractors who are not eligible for DoD PKI certificates but who require certificates to access DoD information systems or to exchange e-mail containing sensitive information must obtain certificates from DoD-approved external PKIs.

Currently, the approved external PKIs are the Interim External Certificate Authority (IECA) and the External Certification Authority (ECA). For more information, including how to obtain certificates, see http://iase.disa.mil/pki/eca.

Back to Questions

38. How do non-US Nationals obtain certificates for use with DoD information systems?

Non-US Nationals who are eligible for DoD PKI certificates should obtain certificates by being issued a CAC or a software certificate, as appropriate.

Non-US Nationals who are not eligible for DoD PKI certificates but who require certificates to access DoD information systems or to exchange e-mail containing sensitive information must obtain certificates from DoD-approved external PKIs.

Currently, the approved external PKIs are the Interim External Certificate Authority (IECA) and the External Certification Authority (ECA). For more information, including how to obtain certificates, see http://iase.disa.mil/pki/eca.

The DoD is participating in NATO discussions for implementing trust in the future in PKIs outside of the IECA and ECA programs.

Back to Questions

DoD PKI PK-Enabling Policy Questions

39. Do PKI and PK-Enabling requirements apply only to the DoD or do they extend to industry?

DoD policies apply to DoD information systems and DoD information. For this reason, DoD partners must obtain and use certificates issued by approved PKIs when interacting with DoD PK-Enabled information systems; accessing DoD sensitive information; or engaging in any other transactions requiring data integrity, confidentiality, or nonrepudiation of DoD information. Specific requirements for individuals to obtain and use certificates are dependent on the actual transactions performed by the individual.

Back to Questions

40. What information systems should be PK-Enabled?

The DoD Instruction 8520.bb requires that private web servers, network login, and e-mail systems be PK-Enabled, and that other information systems perform a business case analysis to determine if PK-Enabling is warranted.

Private Web Servers

Private web servers should be PK-Enabled to use server certificates for confidentiality. This involves each web server obtaining and installing a web server certificate and enabling Secure Sockets Layer (SSL). As a result, all communication between the web server and a web browser is encrypted.

Private web servers should also be PK-Enabled to require client based certificate authentication. This requires the web server to have a certificate and each authorized user of the web server to have an identity certificate. For more information about authentication, see "How are certificates used for authentication to a web server?" There are two important requirements regarding client side PK-Enabling:

- Web servers protecting access to personal information for information-privileged individuals, volunteers, and reservists do not require client certificate authentication, but shall at a minimum require userid and password based authentication.
- Information systems requiring PK-Enabling that include users who are DoD Partners not eligible for DoD PKI certificates shall support certificates issued by DoD approved external PKIs

Network Login

DoD networks required by DoD Directive 8500.1 to authenticate users should perform this authentication using certificates issued by the DoD PKI on hardware tokens. This requires that all individuals with local network accounts have CACs (or equivalent for SIPRNet), card readers and middleware installed on their workstations, and a network system that supports certificate-based login.

E-Mail Systems

E-mail systems should support both digital signature and encryption. Meeting this requirement involves ensuring that both e-mail servers and e-mail clients are compatible with the S/MIME standard.

Sending signed e-mail requires that the sender of the e-mail have a signature certificate that contains the e-mail address of the sender. Although Microsoft Outlook can be configured to ignore the e-mail address contained in the certificate, allowing the sending of e-mail that has been signed with a certificate containing an e-mail address that does not match the sender's e-mail address, unless the recipient of the e-mail has also suppressed this name checking, the signed e-mail will be reported as having an invalid signature when it is read by the recipient.

Receiving signed e-mail requires that the recipient be able to either validate the signature on the e-mail, or view the e-mail with a notice that the signature is not validated (and should therefore be treated as unsigned). For e-mail messages signed using certificates issued by DoD-approved PKIs, the recipient should be able to verify that the certificate was issued by a trusted Certification Authority (CA) and has not been revoked. For e-mail messages signed using certificates issued by non-approved PKIs, the recipient should be able to view the message text even though the signature itself cannot be validated.

Sending encrypted e-mail requires that the sender and all recipients of the e-mail have encryption certificates. The sender must also be able to obtain the encryption certificates for each of the recipients, either from a local certificate store on the sender's workstation or from a directory that the sender's e-mail system can access.

Receiving encrypted e-mail requires that the recipient be in possession of the private key associated with the public key in the certificate used to encrypt the e-mail and that the e-mail client be able to access this private key.

Other Information Systems

Information systems other than web servers, network login, and e-mail systems should assess the capabilities that PK-Enabling can provide to determine if the benefits of PK-Enabling outweigh the costs. For information systems requiring authentication, this business case analysis must be submitted to the Component CIO. For information systems requiring encryption or signature, review by the Component CIO is not required.

Back to Questions

41. Why should information systems use PKI to provide security services?

PKI can provide needed security services for information systems. Primary benefits of Public Key enabling include encryption of information in transit, strong authentication of users, and digital signatures for data integrity and to assist with technical nonrepudiation. For more information, see "Why are usernames and passwords not sufficient for authenticating to web servers?" "How are certificates used for authentication to a web server?" "What is a digital signature?" "What actions must be taken to support non-repudiation of digital signatures?" and "How is PKI used for encryption?"

Back to Questions

42. Why are usernames and passwords not sufficient for authenticating to web servers?

The use of usernames and passwords for accessing web servers has a number of security related issues. One issue is that users are required to remember the username and password for each system that they access. Most users find it impractical to remember a distinct password for each system they access, so they use the same password to access multiple sites. Each site that the user accesses with the same password becomes only as secure as the least secure site. Some examples of poor security at any site follow:

- On the Internet, username and password information is sent through untrusted connections. Any site that does not use encryption is vulnerable to an adversary downloading information and reading usernames and passwords as they are sent from the browser to the web server.
- When accounts are initially created, username and password information must be transmitted from the account creator to the user. If this transmission is not performed out of band, an adversary can determine the username and password information of a legitimate user by intercepting the account creation message.

Another issue with the use of usernames and passwords is that these usernames and passwords must be stored in a centralized database within the information system. If an adversary is able to attack the system and access this centralized information, password cracking tools can be used to gain unauthorized access.

Users access web servers both from government or company provided workstations, which generally have anti-virus and other protections installed, and from home computers, which may not have adequate protective software. If an adversary is able to gain unauthorized access to a home computer, they may be able to use keystroke monitoring to determine username and password information.

The use of certificate-based validation to web servers mitigates these types of problems. Since certificate-based authentication is based on a challenge and response involving the private key that is never sent over the network, a replay attack is not possible. Therefore, if an adversary intercepts communication between a user and an unprotected web server, the adversary does not gain sufficient information to access protected web servers. Since the private key is generated in the presence of the user, and never leaves the control of the user, certificate-based account generation does not require the transmission of password data from the account creator to the user. Instead, once the account creator determines that the user named in the certificate is authorized access, the certificate information can be mapped to the authorizations and the user can be informed that the account is active. The user then accesses the account using the private key already in the user's possession. The centralized database containing authorizations does not contain the private keys necessary to authenticate to the server. While the use of software certificates does not completely mitigate the risk of an adversary gaining access through attacks on home computers since the private key store could be copied from the home computer, the use of hardware tokens significantly decreases this risk.

Back to Questions

43. What is the difference between the DoD PKI Medium-Grade and the Fortezza High-Grade message service?

Fortezza is a form of PKI that, together with the High-Grade Message Service, use government proprietary technology that is not interoperable with any other system. The DoD PKI uses commercial standard technology that is interoperable with almost all PKIs implemented throughout the world. As the defense Message system and the DoD PKI evolve, the DoD PKI will take on the functions of the Fortezza PKI. In the interim, the DoD PKI can be used to digitally sign and encrypt information that requires identification and authentication, integrity, non-repudiation and confidentiality with DoD and non DoD entities who only have access to standard commercial products.

Back to Questions

44. What is a DoD private web server?

On unclassified networks, DoD private web servers are defined as any DoD owned, operated, or controlled web servers providing access to sensitive information that have not been reviewed and approved for public release. In many cases, web servers do not themselves host the information, but act as a mechanism for clients to access information stored in databases or other storage systems. These web servers are still considered to be DoD private web servers and must be PK-Enabled.

On the SIPRNet and other classified networks, DoD private web servers are defined as web servers that provide access to information that require need-to-know control or compartmentalization.

Back to Questions

45. What is a DoD public web server?

A public web server, also known as a publicly accessible web sever, is a web server that is designed for and/or provides information resources to the everyone that may have access to that network. On unclassified networks, this means that all information accessible through that server has been approved for general public release. For the SIPRNet and other classified networks, this means that none of the information accessible through the web server requires need-to-know control or compartmentation.

The physical location of the web server (i.e. behind the Demilitarized Zone (DMZ), within the DMZ, or outside) has no bearing on the designation of the server as being public. Furthermore, the term "publicly accessible" must not be confused with the ability for a limited general public audience to have authorized access to a private web server as defined above. The designation of a web server as private or public rests entirely on the nature of the information available through the server.

Back to Questions

46. Should DoD Components be concerned with DoD Sensitive information on publicly accessible web servers?

Yes. There should never be sensitive information available from publicly accessible web servers.

The DoD "Web Site Administration Policies & Procedures," dated 25 November 1998 and updated 1 November 2002 (see http://www.defenselink.mil/webmasters/security) addresses removal of sensitive information from publicly accessible web sites. Section 4.3.1 states "4.3.1. DoD Web sites containing i) FOR OFFICIAL USE ONLY information, ii) information not specifically cleared and marked as approved for public release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)), or iii) information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, especially in electronically aggregated form, must employ additional security and access controls. Web sites containing information in these categories should not be accessible to the general public."

DoD Directive 8500.1 "Information Assurance," dated 24 October 2002 also contains requirements for protection of DoD Sensitive information.

Back to Questions

47. Does every web server have to be PK-Enabled?

No. DoD public web servers do not require PK-Enabling. Also, DoD private web servers that only provide access to personal information for information-privileged individuals, volunteers, and reservists do not require client certificate authentication, but do require web server certificates. For more information about public and private web servers please refer to "What is a DoD private web server?**"** and "What is a DoD public web server?"

Back to Questions

48. Does the requirement to PK-Enable web servers refer to portal technology?

Yes. If the portal acts as a proxy to applications, provides direct access to restricted information, serves to restrict access to those applications on the back end, or the communication channel initiates and terminates at the web portal than the web portal must be PK-enabled in accordance with the requirements for DoD private web servers. However, if the portal only passes traffic off to other web servers that independently establish secure communication channels directly with the client then the portal may be a DoD public web server. In this case, all web servers behind the portal must be PK-Enabled based on their own status as private or public web servers.

Back to Questions

49. What are the Heads of the DoD Components responsible for with respect to PKI and PK-Enabling?

The Heads of the DoD Components are responsible for planning, programming, and budgeting to support the evolution of the DoD PKI program and to PK-Enable applicable Component information systems. Component Heads are required to develop an implementation plan that details how the Component will implement PKI and PK-Enable information systems.

Component Heads are responsible for ensuring that new COTS and GOTS information systems as well as legacy systems that require PK-Enabling have been tested to ensure interoperability with the DoD PKI, and to report to the DoD PKI PMO what information systems have successfully completed testing. In addition to PK-Enabling Component information systems, Components are responsible for PK-Enabling information systems for Joint programs for which the Component is the executive agent, PMO or equivalent, and to coordinate with other Components and the DoD PKI PMO for interoperability testing of information systems that are used throughout the Department of Defense.

Component Heads are also responsible for coordinating with the DoD PKI PMO to identify requirements for DoD PKI upgrades, information system interoperability testing, and PKI interoperability with external entities.

Back to Questions

50. Do Components have to establish an office for PKI and PK-Enabling responsibilities?

Components are required to provide PKI and PK-Enabling Points Of Contact (POCs) to the DoD PKI PMO. These POCs may be a single office or two distinct offices. This responsibility may be added to an existing office, there is no requirement to establish a distinct office for PKI and PK-Enabling.

Back to Questions

51. Will DoD Components be able to perform DoD PKI interoperability testing internally or does all testing have to be performed at a centralized testing facility?

The DoD PKI PMO is responsible for certifying testing facilities. Services and Agencies may stand up facilities to perform interoperability testing. Each Service or Agency that establishes a testing program will have to coordinate with the DoD PKI PMO to approve the facility.

Back to Questions

52. Who will maintain a list of information systems that have successfully passed DoD PKI interoperability testing?

The DoD PKI PMO is responsible for maintaining and publishing a list of PK-Enabled DoD information systems that have successfully passed DoD PKI interoperability testing. This list is provided to the DoD PKI PMO by the PI-Enabling POCs from the DoD Components, and includes COTS products, GOTS products, and legacy information systems.

Back to Questions

53. What is the intent of the policy statement that the Heads of the DoD Components shall "Coordinate with other Components and the DoD PKI PMO for interoperability testing and PK-Enabling of information systems used throughout the Department of Defense?

The intent is two-fold. First, coordinating interoperability testing across the Department of Defense for commonly used information systems will help to eliminate duplication of effort. The second intent is to ensure that these information systems, which are often COTS products, are tested to meet all of the requirements of the DoD PKI interoperability test plan and that any issues are identified and resolved using the leverage of the Department of Defense. Currently, some of these common products have not been required to undergo PKI interoperability testing because of their common use.

Back to Questions

54. What are Component CIOs responsible for with respect to PKI and PK-Enabling?

Component CIOs are responsible for reporting PKI and PK-Enabling policy compliance status, developing the waiver process for the Component, approving waiver requests in accordance with the waiver process, reporting approved waivers, and approving business case analyses for PK-Enabling of information systems.

Back to Questions

55. When are waivers required?

A waiver is required when an information system that requires PK-Enabling has not yet been enabled in accordance with the Component implementation plan. Waivers will be granted on a temporary basis only.

Back to Questions

56. How are waiver requests made?

Each Component CIO is required to develop a waiver process. Waiver requests should be made according to the Component waiver process. If a waiver is required for an information system that is used by multiple Components, the request should be made to one Component CIO according to the waiver process for that Component, and the Component CIO will forward the waiver to the DoD CIO to request a Department-wide waiver.

Back to Questions

57. For which information systems can a Component CIO approve a waiver request?

Component CIOs can approve or disapprove waivers for all information systems under their purview in accordance with their established waiver process. Waivers will be granted on a temporary basis only. If the information system crosses multiple Components, then the Component CIO must forward the waiver to the DoD CIO to request a Department-wide waiver.

Back to Questions

58. How will information systems that will not be PK-Enabled because there is no business case be handled?

For information systems requiring authentication other than network login or web servers, the system owner shall perform a business case analysis to determine if PK-Enabling is warranted. The business case analysis shall be submitted to the Component CIO for review and approval. If the business case analysis indicates that the information system does not warrant PK-Enabling, no further action is required with respect to meeting the PK-Enabling requirements.

Back to Questions

Implementation Questions

59. What issues have impacted the integration of PKI and PK-Enabling within the DoD?

The scale of the DoD PKI has presented many challenges. For example, the ability to use PKI on a Smart Card for access to networks is limited by COTS technology not accepting standards-based PKI certificates. Also, certificate status checking has been problematic. This is the ability to verify that a certificate is still valid (comparable to a credit card authorization at the point of purchase). The migration from a Certificate Revocation List (CRL), which has grown to a massive unusable size, to alternative standards based COTS technologies for certificate revocation checking is a challenge.

User training, understanding of PKI technology, and resource availability for PK-Enabling of information systems continue to be challenges.

Back to Questions

60. How do I use a CAC

Certificates are stored on the chip embedded in the Common Access Card (CAC). The chip also contains a processor, which responds to two protocols, PKCS#11 and Microsoft CAPI. To use a CAC, the workstation must have a smart card reader installed and must have software installed that enables the interaction between the application and the CAC, called middleware. The installation of smart card readers and middleware is the responsibility of the command that controls the workstation configuration.

Once the reader and middleware have been installed, some applications, including Microsoft Outlook and Microsoft Internet Explorer, require configuration to install the certificates from the smart card into the application. The private keys never leave the card, but the configuration step tells the application that the private key associated with the certificate can be found on the CAC. This configuration is also the responsibility of the command that controls the workstation configuration, but requires that the card be present in the card reader to perform the configuration.

After the workstation is configured, using the CAC involves putting the card in the reader prior to use, and using the user interface provided by the PK-Enabled client application to sign, decrypt, or identify yourself to PK-Enabled information systems. The CAC must be unlocked prior to use by entering the PIN when requested. If the PIN is entered incorrectly four times in a row, the CAC will lock and require a visit to a RAPIDS terminal or a CAC PIN Reset station for unlocking.

Back to Questions

61. How do I read archived encrypted e-mail after I get a new CAC?

Because the private key required to read encrypted e-mail is stored on the CAC, getting a new CAC results in the loss of the key. There are two methods for ensuring access to archived e-mail beyond the expiration date of the CAC. One method is to decrypt all archived e-mail prior to CAC expiration. The second method is to request recovery of the escrowed copy of the private key that is needed to decrypt the archived e-mail. Recovered keys are provided in PKCS#12 software files that must be installed on the workstation to be able to read the archived e-mail.

Currently, key recovery requires the involvement of two Key Recovery Agents and can be time consuming. The DoD PKI PMO is developing an automated key recovery solution that will allow subscribers to recover their own keys without additional personnel, but this capability is not yet operational.

Back to Questions

62. How do I authenticate to a PK-Enabled web server from a workstation that does not have a card reader?

For DoD eligible users, the Common Access Card (CAC) is the primary token for protecting private keys associated with identity, signature, and encryption certificates issued by the DoD PKI. The DoD PKI does support the issuance of software certificates, which may be requested when certificates are required but card readers and middleware are not yet available, however these certificates have less protection for private keys and their use is discouraged.

CAC users that need to have access to PK-Enabled applications from remote locations should be provided the necessary resources to ensure the security of DoD information. For DoD Partners, software certificates may be issued by approved PKIs.

Back to Questions

63. How should DoD Components prioritize PK-Enabling of information systems?

Unclassified networks hosting Mission Assurance Category I (MAC I) information systems should be given highest priority for PK-Enabling. The specific prioritization order for PK-Enabling information systems beyond this requirement is at the discretion of each individual Component. In general, information systems that are most at risk based on the type of information accessible and the community that requires access to this information should be targeted first.

Back to Questions

64. When should PKI be used to encrypt information in transit?

DoD private web servers are required to encrypt information in transit. E-mail may be encrypted in transit if required by other policies.

PKI should also be considered for encrypting information in transit when all of the following are true:

- Encryption of the information is required because of the sensitive nature of the information and the assurance level of the network over which it is being transmitted;
- PKI is approved for encrypting that type of information in that environment; and
- PK-Enabling capabilities are cost effective to implement.

Back to Questions

65. When should PKI be used to encrypt files at rest?

Although PKI may be used to encrypt files at rest, requirements to access encrypted files for both short term and long term should be considered when determining what files to encrypt and what technology should be used for that encryption.

Back to Questions

66. When should PKI be used to encrypt e-mail?

Guidelines for encrypting e-mail will be provided by ASD(NII). Each Component is responsible for developing specific policies for e-mail encryption.

Back to Questions

67. When should PKI be used to digitally sign e-mail?

E-mail requiring data integrity, message authenticity, or nonrepudiation of DoD sensitive information, other than personal information sent by information-privileged individuals, volunteers, or reservists, shall be signed using DoD approved certificates.

Additional guidelines for signing e-mail will be provided by ASD(NII). Each Component is responsible for developing specific policies for e-mail signature.

Back to Questions

68. When should PKI be used to digitally sign documents other than e-mail?

Guidelines for digitally signing documents other than e-mail will be provided by ASD(NII). Each Component is responsible for developing specific policies for digital signatures.

Back to Questions

69. Can PKI be used to secure wireless communications?

Yes. Certificates provide the capability to authenticate users. There are vendors that provide gateways that use certificates to authenticate users to WLANs. The next generation of wireless access points will be more capable of providing these services by implementing the 802.1x standard and WPA.

Back to Questions