What are PKI Certificates?

The PKI framework revolves around the issuance of "certificates" and "private-public" key pairs. A PKI certificate is the digital representation of a physical (paper) certificate. "Physical" certificates (driver's license, passport, identity card, etc.) authorize owners the use of specific services. "Digital" certificates identify and provide you access to PKI security services. A certificate binds an individual's identity to their public key. You will be issued the following three types of PKI certificates:

- **Identity Certificate**
  Used to identify a user to network devices and applications such as web servers.

  The corresponding private key to your identity certificate is used to digitally sign electronic documents. This facilitates authentication and non-repudiation.

- **E-mail Signature Certificate**
  The private key associated with the public key contained in the sender's certificate is used to digitally sign e-mail. Used for authentication to system domains. The sender's public key is used to verify the digital signature on e-mail.

- **E-mail Encryption Certificate**
  Contains recipient's public key, used by senders to encrypt e-mail. The recipient uses the corresponding private key to decrypt e-mail, which facilitates greater security and confidentiality.

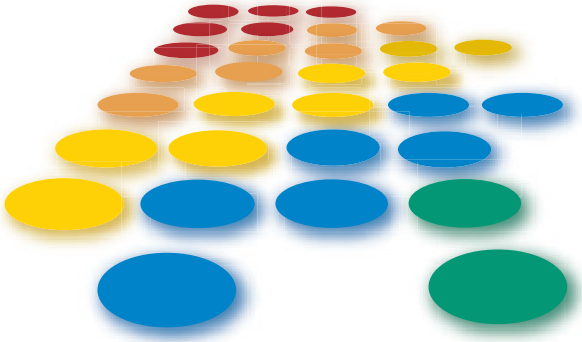
Who Needs PKI Certificates?

- All DHS employees
- Selected DHS contractors

Department of Homeland Security
Identification and Credentialing System
(ICS) Program Office

https://dhscio.net

DHS Access Card (DAC) and Public Key Infrastructure (PKI)



Providing secure information assurance for Department of Homeland Security electronic applications enabled by superior pubic key infrastructure

What is a DAC?

A DHS Access Card (DAC) is the new Department of Homeland Security Identification Card. It is a credit card-sized identity card that contains integrated circuit chips, a magnetic strip, bar codes, and a digitized photo. The integrated circuit chip is where PKI certificates/keys reside.

Users can use the PKI certificates on their DHS Access Card (DAC) to digitally sign e-mail and other documents and to establish secure Internet sessions.

To use PKI certificates a user inserts their DAC into a smartcard reader attached to their computer. Your PKI credentials are made available for use with Public Key enabled applications by unlocking your DAC using your fingerprint and/or entering your 6-8 digit PIN. In addition to standard identity purposes, the DAC will be used for building access. Therefore, users must protect their DACs at all times from access by other people. After all, you wouldn't leave your ATM card and PIN lying on your desk.

Each time a user transfers to another agency, their PKI e-mail certificates must be reissued to match their new e-mail address.

What is PKI?

PKI is our "Electronic Key to the Future." PKI includes a combination of hardware, software, policies, and procedures as well as the ability to authenticate to servers and system domains, protect, and digitally sign electronic mail and documents. PKI verifies identities through the use of digital signatures and certificates. Digital signatures are as legally binding as handwritten signatures.

The Department of Homeland Security (DHS) is implementing PKI to ensure that information is transmitted securely across the Internet. DHS users will be able to log on to their computer, send signed and/or encrypted e-mail, access secure web sites and pass through physical security using their PK-enabled smart card and fingerprint and/or PIN.

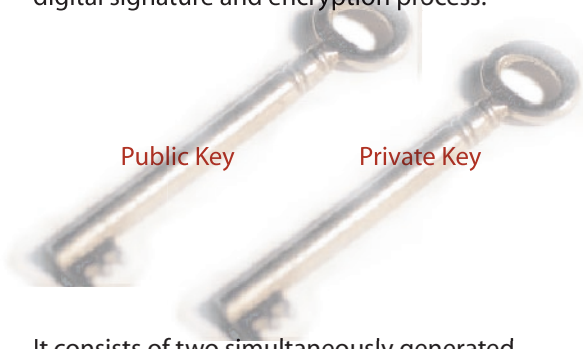
What are PKI security features?

PKI enhances the security of the electronic business that we transact. Security is enhanced through the use of 128-bit encryption and digital signing, both developed by the NSA. In short, PKI satisfies most of our information security needs. PKI minimizes risks with the following security features:

- **Authentication** – a guarantee that e-mail really comes from the person who claims to have sent it. PKI also enables server sites to authenticate user identities before granting access and enables users to verify a server site's identity.
- **Integrity** – a warning if changes were made to the document before the intended recipient receives it.
- **Non-repudiation** – the certainty of knowing that the sender of an e-mail, or signer of a document, cannot later deny having conducted the transaction.
- **Confidentiality** – assurance that information is not disclosed to unauthorized entities (encryption).

How does PKI work?

PKI electronically provides services through the use of a private-public digital key pair, one private and one public, and supports a digital signature and encryption process.



It consists of two simultaneously generated keys using an irreversible mathematical process, making it virtually impossible for anybody to determine the mathematical bond between the two. A key is a digital, computerized code uniquely tied to a user's identity. The two keys are uniquely paired with one another and neither key can be derived from the other. A private key allows a user to place their digital signature on documents and outgoing e-mail, as well as decrypt any encrypted incoming e-mail. PKI-supported web sites can require visitors to authenticate their identities with a certificate prior to allowing them access. This enhances access control to an organization's sensitive information.

Users will use these keys to digitally sign and transmit computer-generated documents and to encrypt e-mail as necessary. As with the key ring in your pocket or in your purse, which contains your car keys and house keys, you will have different sets of keys used for different electronic applications.