

## Public Key Infrastructure (PKI) Technology

### DESCRIPTION

Public Key Technology encompasses the use of two cryptographic keys, a public key and a private key.

Public and private keys are mathematically related. The advent of complexity and speed in modern computer and telecommunications system has driven the need for a more robust and efficient form of cryptography. Public key cryptography, in addition to maintaining privacy and security, has several other security-related attributes, including digital signatures. A digital signature provides proof the originator of the message is authentic. If the originator wants to sign the message prior to sending it to an addressee, the message is passed through a mathematical function (hash function), which provides a summary (hash code) of the message itself. The hash code is then encrypted with the private key and attached to the end of the message. The resultant code constitutes a digital signature. PKI will provide an integrated public key infrastructure that supports a broad range of commercially based, security enabled applications and provides for secure interoperability with the DoD and its federal, allied and commercial partners while minimizing overhead and impact to operations. It will be developed in accordance with the DoD's Defense in Depth, layered information assurance (IA) specifications.

PROCUREMENT PROFILE:	FY00	FY01
<i>Quantity:</i>	<i>0</i>	<i>TBD</i>

### OPERATIONAL IMPACT

PKI is a vital element in achieving a secure Information Assurance (IA) posture for the Defense Information Infrastructure (DII). PKI will support the operating forces and supporting establishment by providing multiple assurance levels in order to enable users to cost effectively and efficiently select appropriate security solutions based on the sensitivity or value of the data, the level of risk, and reliance of the security mechanism on the certificate management information.

### PROGRAM STATUS

The Marine Corps has set up a Marine Corps Registration Authority (RA) at MITNOC. There will be a Local Registration Authority (LRA) located at each Region. The first will be located at MITNOC due to the rapid implementation of several applications such as DTS, EDA, and Marine Corps Manpower application Marine on Line (MOL). The USMC is actively pursuing the aggressive time line set by the DEPSECDEF Memorandum dated 6 May 1999.

### DEVELOPER/MANUFACTURER

TBD