PUBLIC KEYING INFRASTRUCTURE: PKI

Prepared by: James M. Thompson, MAG Aerospace

Public Keying Infrastructure – PKI

Strong cryptography is essential for information security. The NSA's CSfC uses a double encryption architecture within its capability packages to secure 'Red' networks. In order to accomplish this, a key component to all of the CSfC capability packages is the use of Public Keying Infrastructure (PKI). This keystone's criticality had the CSfC take the Key Management Requirements out of the individual capability packages and place them in a standalone document, common to all capability packages.

Normal government-owned encryption devices use symmetric keys where the same key is used on both sides, using a single key for NSA 'type 1' encryptors. With PKI, an asymmetric key is used with both a public key and private keys used. There are six components of PKI.

1. Regulation Authority
2. Certificate Authority
3. Certificate directories
4. Management protocols
5. Certificate Policies (CP)
6. Certificate Practice Statements (CPS) or Procedures

The PKI architecture that a government customer must develop includes these six components starting with a root certificate authority maintained but offline from the network and subordinate certificate authority which provides the keys for servers and clients. Included within the development effort are the CP and CPS which align with RFC 3647 and NIST SP 800-53 version 5 which maps to the CSfC Key Management checklist.

Initially, the Information Assurance Directorate (IAD) specified the use of Suite B cryptographic algorithms in solutions approved for protecting classified and unclassified National Security Systems (NSS). The Suite-B previously specified that "Elliptic Curve Public Key Cryptography. In 2015 the NSA announced that it plans to transition from Elliptic Curve Cryptography to new algorithms that are resistant to attack by future quantum computers. In the interim, the CSfC set the following for classified information:

Transition Algorithms

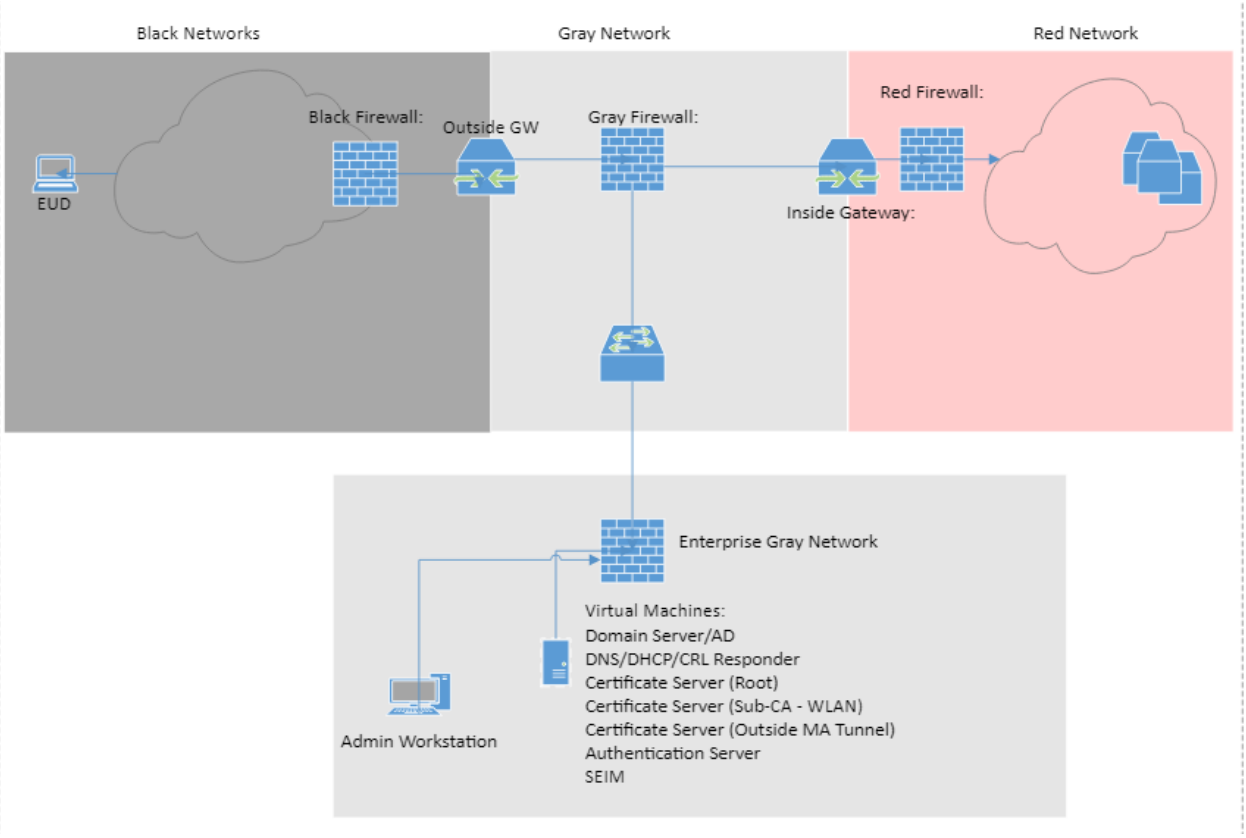
Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

Most people have experienced PKI when using Internet web services when seeing a ‘pop-up’ accepting a certificate. In the DoD, customers use their Common Access Cards (CAC) to access the NIPRnet. The CAC has certificates embedded which are used to authenticate through DoD enterprise servers on the NIPR network. The CSfC capability packages reference three networks – Black, Gray, and Red. The Red network is the classified network being supported which means it has no encryption while the Black network in the transport which requires two encryption tunnels – Outer and Inner. The Gray network terminates one of the encryption tunnels – Outer – therefore has a single encryption tunnel running through it. There needs to be a PKI supporting both these outer and the inner tunnels.

In the NIPR network example above, if an end user connected from a remote location (Black network), the NIPR network would be considered the 'Red' network within a CSfC capability package. One solution would have the end user's machine connect to the 'Gray' network gateway terminating the 'Outside' tunnel using a 'Gray' certificate. The end user would use a second 'Red' certificate to terminate the 'Inside' tunnel to a gateway. This would place the machine on the 'Red network where the user would use their CAC for authentication and logging into NIPR.

Generic MACP Diagram



Generic MACP with WLAN CP