

Position Paper

Department of Defense (DoD) Digital Signatures and Commercial Practices

Digital signature services are fundamental for secure electronic transactions, when there is a requirement to authenticate the parties conducting electronic transactions, and guarantee the integrity of those transactions. A digital signature service requires the choice of an algorithm (i.e., a mathematical equation) for performing the digital signature process, and a supporting infrastructure to provide the electronic "personality" (i.e., public key certificate) used to represent the individual in the signing and verification process. The signature algorithm relies on the infrastructure to provide the trusted association of the public key certificates to the individual users.

Within currently available technology, several algorithm options exist for implementing digital signature to include:

- Digital Signature Standard (DSS), as specified in FIPS 186, and
- Commercial signature algorithms, such as RSA Signature.

DSS is a Federal Information Processing Standard used within the federal government including DoD. Private sector organizations typically have adopted commercial signature algorithms such as RSA. To meet overall DoD objectives for secure electronic transactions, support for both DSS and commercial signature algorithms such as RSA is necessary. The Public Key Infrastructure (PKI) for the DoD, therefore must provide support for multiple levels of assurance and multiple signature approaches, to include both DSS and commercial signature algorithms.

DoD plans to use DSS for electronic transactions within the Department. Commercial signature algorithms (RSA, etc.) are appropriate for achieving interoperability with commercial trading partners. Business Area Managers should consider both DSS and commercial signature algorithms when modernizing.

A DoD-wide PKI will be established to support digital signature services as well as other security services such as encryption throughout the DoD. The National Security Agency (NSA) and Defense Information Systems Agency (DISA) jointly will undertake this responsibility. This PKI will satisfy the requirements of all DoD Business Areas, and provide for interoperability with non-DoD trading partners. To assure interoperability across the full spectrum of DoD requirements and functional areas, the DISA and NSA will establish a Technical Framework for the DoD PKI, defining a comprehensive set of infrastructure services along with implementation