E-SIGNATURE LAWS, REGULATIONS & STANDARDS FOR GOVERNMENT

The following is an overview of relevant electronic signatures laws, regulations and standards that apply to government organizations as well certifications applicable to electronic signatures, PKI and credentials.

LAWS & REGULATIONS

GOVERNMENT PAPERWORK ELIMINATION ACT (GPEA) • http://www.whitehouse.gov/omb/fedreg_gpea2

Signed into law in 1998, GPEA was adopted to encourage the use and acceptance of electronic records and signatures throughout government. The legislation does not prescribe a particular form of electronic signature, rather states that an electronic signature is, "a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message; and indicates such person's approval of the information contained in the electronic message."

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (E-SIGN)

The Federal Electronic Signatures in Global and National Commerce Act (ESIGN) gives legal recognition for electronic signatures and records to satisfy the "in writing" legal requirements for transactions, including disclosures, and permit organizations to satisfy statutory record retention requirements solely through the use of electronic records. ESIGN requires a person's consent to conduct business electronically.

CERTIFICATIONS AND STANDARDS

NATIONAL INSTITUTE STANDARDS AND TECHNOLOGY (NIST) • http://www.itl.nist.gov/fipspubs/fip186.htm

NIST is a US federal agency that develops and promotes standards for digital signatures and e-authentication. 180-3 is the secure hash standard that specifies five algorithms for message digest creation. 186-3 is the digital signature standard used to digitally sign an electronic record or message. FIPS 201-1 is the standard for personal identity verification of government employees and contractors. And last but not least, FIPS 140-2 - a standard that specifies the security requirements that will be satisfied by a cryptographic module used within a software application like electronic signatures.

JOINT INTEROPERABILITY TESTING COMMAND (JITC) • http://jitc.fhu.disa.mil/projects/pki/pke_lab/pke_index.aspx

JITC, operating under the Defense Information Systems Agency, conducts independent interoperability testing of public key enabled applications for use with the DoD Public Key Infrastructure. JITC has awarded twelve certifications to e-SignLive – a process involving more than 300 rigorous tests.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD 12) • http://www.idmanagement.gov/

HSPD-12 is a Common Identification Standard for Federal Employees and Contractors, to improve security and protect personal privacy. The goal is a consistent approach to credential and access management to ensure interoperability. As a public-key enabled software product, e-SignLive solutions can accept FIPS 201-1 compliant digital certificates.

Last updated October 2015