



## Compliance Component

### DEFINITION

<i>Name</i>	Digital Signature
<i>Description</i>	<p>A Digital Signature is a function provided by Public Key Infrastructure (PKI). The process entails transforming a message or data and some secret information held by the sender into a tag called a signature. It provides proof of the source and verification of the integrity of the data.</p> <p>The sender generates a digital signature using his/her private key. The recipient verifies the sender's identity using the sender's public key.</p>
<i>Rationale</i>	The purpose of a digital signature is to provide a means for an entity to bind its identity to data, and to detect unauthorized modifications to data.
<i>Benefits</i>	<ul style="list-style-type: none"> <li>• Digital signatures eliminate the need for transmitting passwords for authentication, which reduces the threat of their compromise</li> <li>• Using a private key to generate digital signatures for authentication prevents an attacker from using the same information to masquerade as another entity and authenticate repeatedly.</li> <li>• Digital signatures provide security for electronic mail, electronic funds transfer (EFT), electronic data interchange (EDI), software distribution, data storage, and other applications that require data integrity assurance and data origin authentication.</li> </ul>

### ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Technical Controls
<i>List the Technology Area Name</i>	Cryptography
<i>List Product Component Name</i>	

### COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

### COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	<ul style="list-style-type: none"> <li>• There are three algorithms suitable for digital signature generation and verification:             <ul style="list-style-type: none"> <li>○ Digital Signature Algorithm (DSA)</li> <li>○ Rivest-Shamir-Adleman, a reversible Digital Signature Algorithm (RSA)</li> <li>○ Elliptic Curve Digital Signature Algorithm (ECDSA)</li> </ul> </li> <li>• Digital signatures require a Public Key Infrastructure (PKI)</li> </ul>
---	--

	<ul style="list-style-type: none"> <li>Users must guard against the unauthorized acquisition of their private keys, because the security of a digital signature system is dependent on maintaining the confidentiality of users' private keys</li> </ul>		
<i>Document Source Reference #</i>	<p>(All found at <a href="http://www.csrc.nist.gov">www.csrc.nist.gov</a>)</p> <p>NIST Federal Information Processing Standards (FIPS) 196, Entity Authentication Using Public Key Cryptography.</p> <p>NIST FIPS 186-2, Digital Signature Standard.</p> <p>NIST FIPS 199, Advanced Encryption Standard (AES) (Nov 2001)</p> <p>ANSI X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).</p> <p>ANSI X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).</p> <p>NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook (Oct 1997)</p> <p>NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government (Nov 1999)</p> <p>NIST SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication (Oct 2000)</p> <p>NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure (Feb 2001)</p>		
<b>Standard Organization</b>			
<i>Name</i>	NIST Federal Information Processing Standards	<i>Website</i>	<a href="http://www.csrc.nist.gov/publications/fips/index.html">www.csrc.nist.gov/publications/fips/index.html</a>
<i>Contact Information</i>	<a href="mailto:inquiries@nist.gov">inquiries@nist.gov</a>		
<b>Government Body</b>			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	<a href="http://www.csrc.nist.gov/publications/fips/index.html">www.csrc.nist.gov/publications/fips/index.html</a>
<i>Contact Information</i>	<a href="mailto:inquiries@nist.gov">inquiries@nist.gov</a>		
<b>KEYWORDS</b>			
<i>List all Keywords</i>	Public key, private key, PKI, DSA, RSA, ECDSA, authenticate, integrity, electronic funds transfer (EFT), electronic data interchange (EDI)		
<b>COMPONENT CLASSIFICATION</b>			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
<b>Rationale for Component Classification</b>			
<i>Document the Rationale for Component Classification</i>			
<b>Conditional Use Restrictions</b>			
<i>Document the Conditional Use Restrictions</i>			
<b>Migration Strategy</b>			
<i>Document the Migration Strategy</i>			

### Impact Position Statement

*Document the Position  
Statement on Impact*

### CURRENT STATUS

*Provide the Current Status)*

*In Development*     *Under Review*     *Approved*     *Rejected*

### AUDIT TRAIL

*Creation Date*

04/13/2004

*Date Accepted / Rejected*

4/13/04

*Reason for Rejection*

*Last Date Reviewed*

*Last Date Updated*

*Reason for Update*