



## Compliance Component

### DEFINITION

<i>Name</i>	Cryptography for VPN
<i>Description</i>	Cryptography for VPN (Virtual Private Network) uses Internet Protocol Security (IPSec) as a method of securing a public network to provide data confidentiality and integrity for remote and mobile users.
<i>Rationale</i>	A public network such as the Internet accessed by a telephone line, cable or DSL, is inherently not secure. A VPN enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.
<i>Benefits</i>	<ul style="list-style-type: none"> <li>• IPSec provides confidentiality and integrity over public network</li> <li>• IPSec minimizes network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping</li> </ul>

### ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Technology 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>• The approved protocol for VPN is the IPSec standard.</li> <li>• The encryption used should be Triple DES or AES.</li> <li>• For very sensitive or critical information, IPSec should be combined with two-factor authentication.</li> <li>• The decision to pass data over a public network should be based on an assessment of the associated risks (see NIST SP 800-30).</li> </ul>
<i>Document Source Reference #</i>	N/A

### Standard Organization

<i>Name</i>	NIST SP 800-30 Risk Management Guide for Information Technology Systems; NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems	<i>Website</i>	<a href="https://csrc.nist.gov/publications/">csrc.nist.gov/publications/</a>
<i>Contact Information</i>	<a href="mailto:inquiries@nist.gov">inquiries@nist.gov</a>		

Government Body			
Name	NIST	Website	<a href="http://csrc.nist.gov/">http://csrc.nist.gov/</a>
Contact Information	<a href="mailto:inquiries@nist.gov">inquiries@nist.gov</a>		
KEYWORDS			
List all Keywords	IPSec, encryption, tunnel, Triple DES, mobile, remote		
COMPONENT CLASSIFICATION			
Provide the Classification	<input type="checkbox"/> Emerging	<input checked="" type="checkbox"/> Current	<input type="checkbox"/> Twilight <input type="checkbox"/> Sunset
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status	<input type="checkbox"/> In Development	<input type="checkbox"/> Under Review	<input checked="" type="checkbox"/> Approved <input type="checkbox"/> 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			