



Compliance Component

DEFINITION

| | |
|--------------------|---|
| <i>Name</i> | Cryptography for Wireless |
| <i>Description</i> | Cryptography for Wireless is a way of securing wireless telecommunications. Wireless is defined as a network or terminal that uses electromagnetic waves, (such as radio frequency, infrared, laser, visible light and acoustic energy) for transmission. |
| <i>Rationale</i> | There is a need for secure electromagnetic access to networks where physical cables are not available and/or feasible. |
| <i>Benefits</i> | <ul style="list-style-type: none"> • Assures the confidentiality of broadcast information • Assures the integrity of broadcast information • Improves secured accessibility |

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> | <p><i>NOTE: Bluetooth technology only radiates up to 10 meters, and is therefore not considered a wireless broadcast device under this compliance component.</i></p> <ul style="list-style-type: none"> • Encryption such as Secure Socket Layer (SSL), Secure Shell (SSH) or IPSec shall be used when broadcasting sensitive or critical information requiring confidentiality, reliability and/or authentication over a public access link, such as wireless. • Wireless connections must comply with NIST Special Publication 800-48 • 802.11i Robust Security Network (RSN) encryption must be activated on the access unit. • The WLAN (Wireless Local Area Network) should use at least a 128 bit key. • An external WLAN must use a Virtual Private Network (VPN) |
|---|---|

| | |
|--|--|
| | <p>when connecting to agency networks.</p> <ul style="list-style-type: none"> • The WLAN must use the Triple Data Encryption Standard (3DES). • The WLAN must use a two-factor authentication scheme. • The WLAN must use Machine Address Code (MAC) authentication or static IP addresses. • The WLAN Service Set IDentifier (SSID) shall not identify the network. Instead, use a long meaningless string of characters or numbers. • The WLAN shall, where appropriate, be set to activate the Broadcast Key Rotation functionality. This will periodically change the communication frequency and impede cracking of the key. |
| <i>Document Source Reference #</i> | |
| Standard Organization | |
| <i>Name</i> | IEEE <i>Website</i> http://www.IEEE.org |
| <i>Contact Information</i> | |
| Government Body | |
| <i>Name</i> | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) <i>Website</i> www.csrc.nist.gov/publications/fips/index.html |
| <i>Contact Information</i> | inquiries@nist.gov |
| KEYWORDS | |
| <i>List all Keywords</i> | WLANs, X.509, Bluetooth, PDA, 802.11, Palm, Pocket PC, Printers, Blackberry |
| COMPONENT CLASSIFICATION | |
| <i>Provide the Classification</i> | <input checked="" type="checkbox"/> <i>Emerging</i> <input type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i> |
| Rationale for Component Classification | |
| <i>Document the Rationale for Component Classification</i> | |
| Conditional Use Restrictions | |
| <i>Document the Conditional Use Restrictions</i> | |
| Migration Strategy | |
| <i>Document the Migration Strategy</i> | |
| Impact Position Statement | |
| <i>Document the Position Statement on Impact</i> | |

CURRENT STATUS

Provide the Current Status)

In Development

Under Review

Approved

Rejected

AUDIT TRAIL

| | | | |
|-----------------------------|-------------------------------|---------------------------------|----------|
| <i>Creation Date</i> | 01/06/05 | <i>Date Accepted / Rejected</i> | 7/12/05 |
| <i>Reason for Rejection</i> | | | |
| <i>Last Date Reviewed</i> | | <i>Last Date Updated</i> | 04/07/05 |
| <i>Reason for Update</i> | To incorporate new technology | | |