



## Encryption: AES versus Triple-DES

All GoodLink messages are encrypted end-to-end using the Advanced Encryption Standard (AES). AES is a Federal Information Processing Standard (FIPS) selected by the U.S. National Institute of Standards and Technology (NIST) for its combination of resistance to attack, ease of implementation, efficiency, and scalable design. All GoodLink clients (Mobitex, Palm OS, and Microsoft Windows Mobile 2003) support Good's implementation of AES.

AES vs. Triple-DES <sup>1</sup>		
	AES	Triple-DES
<b>Description</b>	Advanced Encryption Standard	Triple Data Encryption Standard
<b>Timeline</b>	Official standard since 2001	Standardized 1977
<b>Type of algorithm</b>	Symmetric	Symmetric
<b>Key size (in bits)</b>	192	168
<b>Speed</b>	High	Low
<b>Time to crack</b> (assume a machine could try 255 keys per second - NIST)	149 trillion years	4.6 billion years
<b>Resource consumption</b>	Low	Medium

*"AES can encrypt data much faster than Triple-DES, a DES enhancement which essentially encrypts a message or document three times."*<sup>1</sup>

<sup>1</sup> Source: NetworkWorldFusion, Resource Links/Encyclopedia