



<b>Company</b>	<b>AKCode LLC</b>
<b>Product/Component</b>	<b>Cavern – Secure Channel Agent</b>
<b>Product Number</b>	AKT4003
<b>Description</b>	<p>Cavern is a client-server software package that encrypts data for transport through a public communication line.</p> <p>The client software encrypts the data before sending it across the network. The data is decrypted by the Cavern server; located on the other side of the public communication line, and once decrypted it is sent to the intended receiver. The receiver does not need to be operating Cavern to receive the secured data, but should be on a private/secure network to ensure secure transport of the data.</p> <p>Cavern is the only software program to secure legacy applications without any modifications of existing software or hardware.</p> <p>Cavern is Simple, Reliable and Secure.</p>
<b>Features</b>	<ul style="list-style-type: none"> <li>➤ Anonymous Key Technology (AKT)</li> <li>➤ Easy to use administrative functions</li> <li>➤ Encrypts any data transported over a specified port</li> <li>➤ Provides biometrically authenticated and encrypted data through the Public Internet for transparent, secure data submission and retrieval</li> </ul>
<b>Benefits</b>	<ul style="list-style-type: none"> <li>➤ Encrypts any file type</li> <li>➤ The Enterprise determines which TCP ports to secure</li> <li>➤ Supports anonymous key negotiation via the UIS PPP protocol. This is analogous to establishing a SSL session with a server</li> <li>➤ Cavern Server supports Windows 2000/2003 Server</li> <li>➤ Cavern Client supports Windows 98SE/2000/XP</li> <li>➤ Supports Smart Cards and Biometric Authentication Capabilities</li> <li>➤ The receiver does not require Cavern to decrypt the incoming information</li> <li>➤ Utilizes the new AES (Advanced Encryption Standard) symmetric encryption algorithm</li> <li>➤ Deployable in global implementations</li> <li>➤ AKT protects information on-site and while in-transit</li> <li>➤ No transfer of public keys or management of private keys</li> </ul>
<b>Certifications</b>	<ul style="list-style-type: none"> <li>➤ FIPS 140-2 Certificate No.339</li> <li>➤ AES Algorithm Validation Certificates No.38 and 47</li> <li>➤ SHS Algorithm Validation Certificates No.128 and 142</li> <li>➤ <a href="http://csrc.nist.gov/cryptval/140-1/1401val2003.htm">http://csrc.nist.gov/cryptval/140-1/1401val2003.htm</a></li> </ul>

The National Institute of Standards and Technology (NIST) has certified that the current implementation of the AKT Cryptomodule will yield a minimum key strength equivalent to 10 random characters and a maximum key strength equivalent to 32 random characters. AKT does not use SSL and does not require PKI; however, AKT can fully supplement an existing PKI system. The current AKT Cryptomodule supports biometrics for both authentication and to strengthen the key.

