



EZ Child ID is the system of choice for Law Enforcement, US Military, and Department of Home Land Security. We are often asked about the security of our software. We use the same process that was adopted by the US Department of Defense. We overwrite the child id file using randomly generated data. This is done using a method which bypasses any caching and writes directly to the disk. We do this a total of 3 times. After overwriting the file 3 times, we change the file size to 0, and then rename the file. The file is given a random name, and each time we rename it - the file name is shortened by 1 character. When the filename is only 1 character long, we then delete it from the hard disk and it is unrecoverable.

We have recently added a new option to our software by delivering you child's information to you iPhone or Android phone via our new EZ Child ID Mobile App. Our EZ Child ID software, packages your child's information in an AES-256 encrypted format and transmits the package to the EZ Child ID Mobile App via an encrypted router. Your information is never on the web. It is only stored on the local secure router for a maximum of 2 hours. The only way to access the information on the router is to enter your child's 3 initials as well as their birthday in Month/Day/Year format. After two hours, your children's data is securely deleted from the server using Department of Defense data deletion standards mentioned above. The AES-256 Standard has been adopted by the U.S. government and is now used worldwide. The bottom line? No one will be breaking your encrypted data on an EZ Child ID system.

#### ***More information on AES-256 encryption***

*AES-256 is a key generation method used to securely encrypt your data and prevent unwanted access to your files. But the real question is how safe is AES 256bit encryption really?*

*When referring to AES-256bit encryption, we are actually referring to the key that is generated when encrypting your data. The data itself is secured by the software by creating a 'key' that uses 256bit encryption to unlock that data. The math behind AES-256 is fairly straight forward, but very important to understand as it relates to the real world.*

#### ***The Math***

*A 256bit encryption is the mathematical equivalent of  $2^{256}$  key possibilities. To put that into perspective,  $2^{32}$  is about 4.3 billion, and it keeps growing exponentially after that. What does this mean though? Well simply put, let's say hypothetically all the super computers in the world (the ultimate brute force attack) decided to group up and tasked themselves to decrypt your AES-256 key so they could access your data. Assume they could look at  $2^{50}$  keys per second (which is approximately one quadrillion keys/second – a very generous assumption). A year is approximately 31,557,600 seconds. This means that by using the one billion super computers required to do this, they could check about  $2^{75}$  keys per year. At this rate it would take these computers  $2^{34}$  years (the age of our universe) to look at less than .01% of the entire key possibilities. The bottom line? No one will be breaking your encrypted data on an EZ Child ID system.*

If you have further questions please call our office and we will be happy to help.

*Sincerely,*

*John Wisniewski*

*John Wisniewski  
President*

**EZ Child ID.com, 34900 Plymouth Rd, Livonia, MI 48150 734-838-9800**