

Re: Thermite type cutting rods

Source: <http://sci.tech-archive.net/Archive/sci.astro.amateur/2007-08/msg02096.html>

- *From:* "Pete C." <aux3.DOH.4@xxxxxxxx>
 - *Date:* Wed, 29 Aug 2007 00:26:33 GMT
-

the LE KEY = Your Key.

So, because they have a separate but equivalent key, they are claiming to be your emergency backup key, like a key left with a neighbor.

People who have no idea how computer systems work will think like that sounds like a reasonable thing.

Like a "good faith attempt to balance...".

Now picture it being YOUR business.

You have a cryptographic key that needs to be protected.

The key itself is a big number you can't memorize.

The key itself is protected by a (MD5-like) password to unlock access to it. That means the password can be as long a thing as you'd like to type in, not merely a short password. As long as you can remember it.

This is standard...MIT's Kerberos and Phil Zimmerman's PGP use a password to unlock the cryptographic key.

So, how do you back up the key without GAK?

In other words, what do all companies do for this situation now?

A situation that applies to all company data whether or not it is encrypted.

A situation that has existed since the invention of the computer.

Simple.

You back it up.

Make backups of the key.

You can start by making your own key copy using off-site secure storage backup.

Re: Thermite type cutting rods

Several authorized people can have a copy of the key, and they can each use their own password to get access to the key.

The key is backed up not only by being on several different machines, it is also backed up in the off-line backups for these machines. After JUST ONE WEEK, you'll have 24 total copies of the key ($3 + 3*7$). After the first month: 214 copies.

The government somehow thinks you'll clamor for THEM to backup your key by giving them a copy of the key, and if you lose all of yours... contact the Federal Secretary of Lost Keys.

And for this great benefit, they want you to give them Key Recovery access to your cryptographic key.

We know what Key Recovery means...