

Article ID:1103
Published date: 22/2/2005
Revision: 1.0

Subject: How is eToken affected from SHA-1 attack?

Classifications: RTE

Information: Responding to the SHA1 attack issue which was raised at:
http://www.schneier.com/blog/archives/2005/02/sha1_broken.html

How is eToken affected by the SHA1 attack?

1. The meaning of attack is that you may crack Hash not within 2^{80} , but around 2^{68} . It is very important in terms of cryptography, less important in real life.
2. The second meaning is that it may be predictor of even more serious attack.
3. Today the entire world uses either SHA-1 or MD5 with digital signatures. SHA-1 is still better than MD5.
4. You may implement better algorithm (there are known algorithms), such as SHA-256 or SHA-512. The question is who you will be compatible with? In the future we might implement them – they will get more using due to the fact that SHA-1 is broken and the implementation effort is small. But within token it doesn't seem suitable.

Key words: SHA1