



April, 2009

Dear System Integrator, dear Partner,

This letter serves to inform you on alleged security issues with respect to our HITAG 1 and 2 product families.

We need to assume that – based on a publication of the HITAG 2 cipher at the FSE 2008 conference - a group of researchers are currently reverse engineering our HITAG 2 chips and are trying to discover the entire encryption algorithm of these chips.

NXP expects that this research group will continue their work until the point that the full algorithm including attack tools will become publicly known. Although there are currently no indications, we need to consider that the same may apply to HITAG 1.

Please note, that this does not have any impact on applications which are not security sensitive, such as animal ID, asset management and industrial production control.

Although there is no public information available yet, we feel it is appropriate to inform you about any measures to be taken to minimize the possible impact of such eventuality.

Should the full algorithm become publicly available, the security of systems using the HITAG 1 and 2 families would become dependent on the secrecy of the keys only. It is our understanding that in well-designed systems, such keys are different per card and are updated on a regular basis.

By eavesdropping on the communication between a legitimate card and a legitimate reader, a hacker could possibly get access to a plain text / cipher text combination. As you know, the keys of the HITAG 1 and 2 are 32, respectively 48 bit long. With the full crypto algorithm and plain text/cipher text combinations available, such key length would allow for a “brute force” attack. However, it is more likely that cryptographic attacks will be found in due time that are more efficient than this.

Although we trust that you have implemented in your systems effective mechanisms to detect fraudulent cards (which we understand is possible in a number of ways), we nevertheless believe it is appropriate to inform you about our investigations into scenarios how end to end security systems can be protected. An Application Note (AN155010) explaining this, is available from NXP under the following URL: http://www.nxp.com/infocus/topics/secure_mifare/. In addition, we would expect you to assess whether your systems would need any additional security measures in light of the above.



Whether the achieved level of security is acceptable or not depends on the assets to be protected which only the system integrator and his customers can determine. Nevertheless NXP does not recommend the use of the HITAG family in security sensitive applications like access management for buildings and properties. In these applications we recommend the use of our products MIFARE DESFire EV1 or SmartMX, which have received Common Criteria Certification, or the upcoming MIFARE Plus which is targeted to receive Common Criteria Certification as well.

NXP's expertise is the design and manufacturing of ICs. We do not design end to end security systems, which is typically the responsibility of system integrators. If you would like to discuss this matter, we will be happy to support you.

If you have any questions or like to be kept informed about the developments in this matter, please contact us at [hitag@nxp.com].

Sincerely yours

The NXP HITAG team

NXP Semiconductors Austria GmbH Styria
Mikron Weg 1, 8101 Gratkorn, Austria
www.nxp.com