

## Statement

NXP would like to respond to reports following a recent presentation by a research group at the 24th congress of the Chaos Computer Club in Berlin where it was claimed there were security flaws found in one of NXP's chips, of a similar type as used in the Dutch Transport system.

NXP would like to clarify that the claims are restricted to obtaining only part of the cryptographic algorithm. As such this does not breach the security. The applications integrate the encryption of the chip as only one part of an end-to-end security system, comprising multiple layers each individually contributing to the total system security. In practice, systems with multiple layers of end-to-end security have the means to detect tampered cards and take appropriate measures within a short timeframe. Even if one layer were to be compromised, other layers will stop the misuse.

The chip in question is one of a family of ICs for contactless cards applications but not - as erroneously referred to in the presentation - targeting ePassport, traditional banking or car security applications.

NXP would also like to point out that the work to obtain part of the cryptographic algorithm has been undertaken over a significant period of time by highly skilled researchers. These substantial efforts are claimed to have led to discovering a part of the algorithm. Another element of the security of the chip, the keys, have not been found and it also has to be realized that those keys are not the same for all cards.

NXP nevertheless takes these claims seriously and is investigating the claims that are made. To this end, NXP aims to meet the research group in the near future to establish an open dialogue and hear in more detail the claims that have been made. NXP will continue to communicate with the media, partners and customers on this topic if there are any significant developments.

NXP will continuously develop encryption systems that meet the moving security requirements of the various applications.