HID

611 Center Ridge Drive
Austin, Texas 78753 USA

FREE +1 800 237 7769
MAIN +1 512 776 9000
FAX +1 512 776 9630

November 1, 2018

HID Statement for IPvM

HID Global has been proactively working to inform and educate access control customers about the importance of migrating away from vulnerable credentials, including 125 kHz technology. The vulnerability inherent in 125 kHz credentials is a known issue that we have been responsibly disclosing to physical access control customers on a regular basis for years. HID has already successfully driven a significant shift in the market from 125 kHz credentials to more secure technology.

HID has been upfront about the vulnerabilities associated with legacy technologies for physical access control, equipping customers to make informed decisions about their own implementations and pace or timeline of conversion. However, we realize that there is more work to be done, as 125 kHz represents approximately 40% of the global physical access control credential market. Until there is a more substantial market shift away from the technology, we prefer that customers source it from a trusted partner.

While enabling choice with multi-technology readers and aggressive promotion of modern technology, HID is leading the shift to more secure credentials by providing incentives for our customers to migrate on their own timelines. **Ultimately, HID aims to help our entire customer base upgrade to holistic, secure smart card and/or mobile credential solutions.**

To increase awareness about the need to upgrade vulnerable credential technology, HID has continually demonstrated to customers how an attacker can use the vulnerabilities to gain unauthorized access. Moreover, HID has posted alerts online about the vulnerabilities of legacy credential technology, such as HID's seminal blog post dating back a few years ago, "Best Practices for Safeguarding Against Vulnerabilities of Legacy Systems."

HID believes that **all** credential vulnerabilities should be addressed; not only 125 kHz. It is worth noting that, while 125 kHz proximity credentials make up a large portion of the installed base, the vast majority of high frequency 13.56 MHz contactless smart cards are deployed in a manner that makes them open to the exact same vulnerabilities. Common vulnerabilities include the following:

- Using CSN/UID unauthenticated read that can be cloned/spoofed with similar tools
- Using contactless smart card technology with known vulnerability that can be cloned/spoofed with similar tools
- Using standard/default keys for secure sector reads

It is our objective at HID to address these common technology and deployment mistakes and establish security best practice as common protocol.