



INFORMATION ASSURANCE DIRECTORATE



“INFORMATION ASSURANCE LEADERSHIP FOR THE NATION”

**(U) INFORMATION ASSURANCE
(U) ADVISORY NO. IAA-014-2012**

Date: 01 November 2012

SUBJECT: (U) Cryptographic Weakness in Certificates Generated on Oberthur v5.2 Smart Cards

1. (U) The National Security Agency’s (NSA) Information Assurance Directorate (IAD) conducts continuous monitoring and analysis to ensure the integrity of the components of National Security Systems. As a result, IAD has identified a flaw in the Oberthur v5.2 (and variant) Smart Card, which results in public keys that do not satisfy the requirements of the Digital Signature Standard (as specified in FIPS PUB 186-3 and its predecessors).
2. (U) Not all Oberthur Smart Card products are affected by this flaw. The affected products include the Oberthur ID-One COSMO 64, v5.2 and v5.2a
3. (U) IAD recommends that all users of Oberthur Smart Card products engage with the vendor to determine if cards in use are affected by this weakness. Visual inspection to determine the variant of the card used is not always possible or effective. Once identified, organizations using the affected cards are encouraged to transition to unaffected hardware as soon as possible.
4. (U) Questions concerning this Advisory should be directed to the NSA Information Assurance Customer Advocate Office at 410-854-4790 or (410) 854-4200.