ISO/IEC JTC 1/SC 27 **N19020**

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	Press Release
TITLE:	**ISO/IEC JTC 1/SC 27 STATEMENT ON OCB2.0 -- -- Major weakness found in a standardised cipher scheme (ISO/IEC 19772:2009-02, 1st ed)**
SOURCE:	**SC 27/WG 2 Convenor, Takeshi Chikazawa**
DATE:	2019-01-09
PROJECT:	
STATUS:	This document is being circulated within SC 27 for information.
ACTION:	**INFO**
DUE DATE:	
DISTRIBUTION:	P-, O, and L-Members, L. Rajchel, JTC 1 Secretariat J. Alcorta, ITTF A. Wolf, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors
MEDIUM:	http://isotc.iso.org/livelink/livelink/open/jtc1sc27
NO. OF PAGES:	1 + 1

ISO/IEC JTC 1/SC 27 STATEMENT ON OCB2.0

-- Major weakness found in a standardised cipher scheme --

7th January 2019

ISO/IEC 19772:2009 'Authenticated encryption' describes a number of ways in which a block cipher algorithm, a very widely used type of cipher, can be used to protect the confidentiality and integrity of a message using a secret key (i.e. a secret value known only to the message sender and intended recipient). Message confidentiality is guaranteed by encrypting the message in such a way that only someone with the secret key used to encrypt it can learn any of its content. Message integrity is guaranteed by adding a tag to the message which can be checked by the intended recipient; the tag will fail the check if any of the message is changed, and a new tag cannot be calculated without knowing the secret key.

One of the techniques standardised in ISO/IEC 19772 is known as OCB 2.0. Very recently, two Japanese academics, Akiko Inoue and Kazuhiko Minematsu, have shown that OCB 2.0 is seriously flawed, and in certain circumstances does not guarantee message integrity. This unexpected finding prompted a flurry of new research, and two other academics: Bertram Poettering (from the UK) and Tetsu Iwata (from Japan), have now shown that message confidentiality is also not guaranteed. This means that OCB 2.0 should no longer be used. Moves are under way to remove it from the international standard.