

## NSA zmienia klucze

<http://ipsec.pl/kryptografia/2009/nsa-zmienia-klucze.html>

Jeśli kogoś interesują wewnętrzne procedury stosowane w amerykańskich agencjach rządowych do przetwarzania informacji niejawnych to drobny wgląd w ich funkcjonowanie można znaleźć w opublikowanej niedawno przez Cryptome [ja href="http://cryptome.org/dodi/nsa-rekey.pdf"](http://cryptome.org/dodi/nsa-rekey.pdf) i instrukcji wymiany kluczy kryptograficznych w urządzeniach STU-III [i/a](#).

Instrukcja zaleca aktualizacje listy anulowanych kluczy (CKL) w związku z tym, że "NSA otrzymała znaczna liczba zgłoszeń o kompromitacji" urządzeń STU-III. Seria [ja href="http://en.wikipedia.org/wiki/STU-III"](http://en.wikipedia.org/wiki/STU-III) i [STU-III](#) [i/a](#) to stosowane od końca lat 80-tych urządzenia takie jak telefony i faksy, wyposażone w sprzętowy moduł szyfrujący implementujący niejawne szyfry oraz mechanizmy wymiany i anulowania kluczy kryptograficznych. W tym kontekście "kompromitacja" może oznaczać fizyczna kradzież urządzeń, w związku z czym NSA zaleca uruchomienie (półautomatycznej) procedury aktualizacji listy kluczy unieważnionych.

<http://cryptome.org/dodi/nsa-rekey.pdf> <http://en.wikipedia.org/wiki/STU-III> <https://www.keysupport.net/frontpage>  
(jawny serwis z poradnikami dla użytkowników STU-III)

Innym ciekawym dokumentem, który niedawno pojawił się na Cryptome jest dokument poświęcony [ja href="http://cryptome.org/dodi/dss-siprnet.pdf"](http://cryptome.org/dodi/dss-siprnet.pdf) i DSS Secret Internet Protocol Router Network (SIPRnet) [i/a](#), czyli niejawnej, rządowej sieci IP wykorzystywanej przez rząd USA.