

# Wojskowy Instytut Łączności - Państwowy Instytut Badawczy

<https://www.wil.waw.pl/wil/oferta/badania-i-rozwoj/zaklad-kryptologii/17627,Zaklad-Kryptologii.html>  
2021-11-29, 00:25

## Zakład Kryptologii

Kierownik - dr inż. Robert Wicik  
tel. 261 885 550

Dostarczanie wymaganych przez ustawę urządzeń i narzędzi kryptograficznych oraz kompletnych systemów ochrony informacji niejawnych.

Pełny cykl opracowania: począwszy od prac badawczo-rozwojowych, poprzez certyfikację typu i zgodności, po produkcję i wsparcie przy wdrożeniu.

### Kryptografia i kryptoanaliza

- o oryginalne algorytmy i protokoły kryptograficzne, dopuszczone do ochrony informacji o najwyższych klauzulach tajności
- o analizy bezpieczeństwa algorytmów kryptograficznych i systemów ochrony informacji

### Urządzenia kryptograficzne

- o oryginalne konstrukcje urządzeń kryptograficznych, przeznaczonych do ochrony informacji niejawnych
- o sprzętowe moduły szyfrowania z kryptografią narodową i interoperacyjną
- o oryginalne konstrukcje identyfikatorów użytkowników i elektronicznych nośników danych kryptograficznych
- o sprzętowe generatory ciągów losowych
- o sprzętowe moduły generacji i zabezpieczenia kluczy

### Systemy zarządzania danymi kryptograficznymi

- o podsystemy planowania, generacji i dystrybucji danych kryptograficznych, w tym kluczy
- o podsystemy monitorowania i zarządzania urządzeniami kryptograficznymi
- o podsystemy infrastruktury klucza publicznego

Uzyskane w ostatnich latach certyfikaty ochrony kryptograficznej

<i>Nazwa urządzenia lub narzędzia kryptograficznego</i>	<i>Nr certyfikatu typu</i>	<i>Klauzula chronionych informacji</i>
---	----------------------------	--

<p>LAWENDA - system ochrony informacji w sieciach radiowych.  Radiowy Moduł Kryptograficzny wraz z identyfikatorem ID-RMK, Dystrybutor Danych Kryptograficznych wraz z identyfikatorem ID-DDK, Polowa Stacja Planowania Generacji i Dystrybucji Danych Kryptograficznych wraz z identyfikatorami ID-u oraz ID-S</p>	<p>21/2020</p>	<p>ZASTRZEŻONE,  NATO RESTRICTED,  RESTREINT UE /  EU RESTRICTED</p>
<p>RUMIANEK -system ochrony informacji w sieciach ISDN.  Terminal BRI ISDN typ RUMIANEK-BRI, Interfejs kryptograficzny PRI ISDN typ RUMIANEK-PRI wraz z zestawem stacji planowania, generacji, ładowania i dystrybucji danych kryptograficznych oraz bankami danych kryptograficznych</p>	<p>58/2017</p>	<p>TAJNE,  NATO/EU CONFIDENTIAL</p>
<p>Sprzętowy generator ciągów losowych SGCL-1MB</p>	<p>143/2016</p>	<p>ŚCIŚLE TAJNE</p>