



# PGP® Command Line 9.6

Szyfrowanie danych przetwarzanych masowo, transferowanych i archiwizowanych

Part of the PGP® Encryption Platform

## Zabezpieczenie transferu i archiwizacji dużych plików danych

PGP Command Line umożliwia administratorom automatyczne zabezpieczanie transferu lub backupu dużych ilości danych, zapewniając zgodność z regulacjami dotyczącymi bezpieczeństwa informacji.

PGP Command Line chroni dane:

- Przesyłane do i z oddziałów firmy, partnerów lub klientów w ramach sieci wewnętrznych lub przez Internet.
- Składowane na serwerach, do których ma dostęp nieautoryzowany personel.
- Przesyłane do zewnętrznych centrów danych, gdy pojawia się ryzyko wycieku lub kradzieży danych.

## Automatyzacja bezpieczeństwa informacji biznesowej

PGP Command Line pozwala organizacji:

- W prosty sposób zintegrować bezpieczeństwo informacji z istniejącymi systemami.
- Zapewnić, że poufne dane są chronione silnymi algorytmami szyfrowania, niezależnie od tego, gdzie są składowane.
- Rozszerzyć dotychczasową infrastrukturę i współpracować z partnerami używającymi kluczy OpenPGP, certyfikatów X.509, PGP Universal™ Server i serwerów kluczy PGP.
- Zachować dostęp do zaszyfrowanych danych w przypadku utraty klucza, dzięki technologii PGP Additional Decryption Key (ADK).

## Element platformy szyfrującej

PGP Command Line może współpracować z innymi aplikacjami będącymi częścią platformy szyfrującej PGP® Encryption Platform, w tym PGP® Desktop, PGP® Whole Disk Encryption i PGP Universal Server oraz z usługami PGP Global Directory. Aplikacja PGP Command Line jest w pełni kompatybilna ze standardem OpenPGP.

## Korzyści w firmie

### Ochrona danych bez programowania

- Funkcje szyfrowania mogą być szybko zaimplementowane w istniejących systemach bez konieczności tworzenia nowego oprogramowania.

- Administratorzy wykorzystują znane już techniki tworzenia skryptów wsadowych do wdrożenia rozwiązania i nie muszą uczyć się nowych technik programowania.

### Zabezpieczony dostęp do danych

Opatentowana technologia PGP Additional Decryption Key (ADK) zapewnia bezpieczny dostęp do zaszyfrowanych danych w przypadku zgubienia klucza szyfrującego lub gdy taki dostęp jest wymagany przepisami prawa.

## Korzyści dla partnerów

### Ochrona sieci partnerów i ochrona łańcuchów dostaw

- Wsparcie wielu platform opartych na systemach operacyjnych Microsoft Windows i UNIX.
- Łatwa integracja nowych funkcji mocnego szyfrowania z systemami komputerowymi u partnerów bez konieczności tworzenia nowego oprogramowania.

### Wsparcie dla małych firm

PGP Command Line umożliwia bezpieczny transfer danych „ad-hoc” do partnerów, którzy nie mają wdrożonego oprogramowania szyfrującego poprzez tworzenie samorozszyfrowujących się archiwów (PGP® Self Decrypting Archives).

## Cechy produktu

### Integracja z innymi aplikacjami

Funkcje szyfrowania, elektronicznego podpisywania i bezpiecznego usuwania plików oferowane przez PGP Command Line można łatwo zaimplementować do istniejących systemów. Wywołanie funkcji produktu PGP Command Line może się odbywać z poziomu:

- Popularnych języków skryptowych, min. PERL, Shell Script, plików wsadowych Windows
- Aplikacji stworzonych w różnych językach programowania

### Wszechstronne wsparcie dla profesjonalnych platform

Produkt PGP Command Line jest dostępny dla systemów Microsoft Windows i UNIX oraz dla IBM® iSeries™ i zSeries™.

# PGP® Command Line 9.6

## Szyfrowanie danych przetwarzanych masowo, transferowanych i archiwizowanych

### Archiwa PGP Zip

- Kompatybilność z różnymi systemami operacyjnymi
- Kompatybilność z PGP Desktop, PGP Whole Disk Encryption i klientami PGP NetShare

### PGP Self-Decrypting Archives

Zaszyfrowane pliki i foldery mogą być spakowane w pojedyncze samorozszyfrowujące się archiwa– (SDA). Archiwa SDA mogą być tworzone i uruchamiane pod każdym systemem operacyjnym wspieranym przez PGP Command Line.

### Bezpieczne usuwanie plików

PGP Command Line zawiera funkcję bezpiecznego i trwałego usuwania plików poprzez nadpisanie danych.

### Integracja z usługami katalogowymi

PGP Command Line może wyszukiwać klucze OpenPGP w zasobach PGP Universal Server, PGP Global Directory i serwerów kluczy PGP. Certyfikaty X.509 mogą być wyszukiwane w katalogach zasobów PGP Universal Server oraz LDAP v3.

### Zaawansowane zarządzanie kluczami – podział kluczy

Aby wyeliminować możliwe nadużycia ze strony administratorów, PGP Command Line umożliwia dokonanie podziału klucza szyfrującego i określenie minimalnej liczby posiadaczy jego części wymaganych do autoryzacji.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners

## Specyfikacje techniczne

### Wspierane systemy operacyjne

- Windows Vista (wszystkie edycje 32-bitowe)
- Windows 2003 SP1
- Windows XP SP2 (edycje 32 i 64-bitowe)
- Windows 2000 SP4
- HP-UX 11i lub wyższy (tylko PA-RISC)
- IBM AIX 5.2 lub wyższy
- RedHat Enterprise Linux 3.0 lub wyższy (x86)
- Sun Solaris 9 (tylko SPARC)
- Fedora Core 3 lub wyższy (x86\_64)
- Apple Mac OS X 10.4 lub wyższy (Universal Binary)

### Serwery usług katalogowych

- LDAP
- PGP Universal Server
- PGP Global Directory
- Serwery kluczy PGP

### Formaty kluczy publicznych

- OpenPGP RFC 2440
- X.509 v3

### Algorytmy kluczy symetrycznych

- AES (do 256 bitów)
- CAST5
- 3DES
- IDEA
- Twofish
- Blowfish\*
- Arc4 (128 bitów)

### Algorytmy kluczy publicznych

- Diffie-Helman (do 4096 bitów)
- DSA (1024 bity, weryfikacja do 3072 bitów)
- RSA (do 4096 bitów)

### Algorytmy hash

- SHA-1, SHA-256
- SHA-384, SHA-512
- MD5
- RIPEMD-160

### Algorytmy kompresji

- Zip
- BZip2
- ZLib

*(aktualne dane techniczne produktu znajdują się na stronie [www.pgp.com/products/pgp\\_commandline/servers/tech\\_specs.html](http://www.pgp.com/products/pgp_commandline/servers/tech_specs.html))*

\*) Wsparcie Blowfish jest ograniczone do rozszyfrowywania wiadomości zaszyfrowanych przy użyciu tego algorytmu lub szyfrowania według istniejących kluczy, które określają Blowfish jako preferowany rodzaj szyfrowania



Veracomp jest wyłącznym dystrybutorem rozwiązań PGP na terenie Polski. Prowadzi sprzedaż wyłącznie za pośrednictwem Partnerów handlowych.  
[www.veracomp.pl/pgp](http://www.veracomp.pl/pgp)  
tel. (12) 25 25 555, fax: (12) 25 25 500

