



**SEPPMAIL**  
SWISS E-MAIL SECURITY

# KARTA PRODUKTU

## Typowe problemy:

Przedsiębiorstwa chronią swe dane firmowe przed wrogimi atakami i ingerencjami za pomocą zapór, systemów antyspamowych i antywirusowych oraz rozwiązań z użyciem haseł jednorazowych. Jednak pracownicy, korzystając z poczty elektronicznej, przesyłają informacje firmowe - także wrażliwe dane poufne - na ogół w formie otwartej i bez ochrony.

**PRZESTRZEGANIE PRAWA:** Przy ustawowych zobowiązaniach według SOX, HIPAA, Basel-II, PCI itd. w przypadku ich nieprzestrzegania istnieje podwyższone ryzyko odpowiedzialności.

**OSZCZĘDNOŚĆ KOSZTÓW:** Dzięki cyfryzacji procesów biznesowych koszty można znacznie obniżyć - np. przy wysyłaniu miesięcznych rozliczeń płacowych lub specyficznych danych osobowych.

**BEZPIECZNA KOMUNIKACJA:** Klienci, dostawcy i partnerzy biznesowi oczekują przy wymianie wrażliwych danych komunikacji bezpiecznej i zaszyfrowanej.

**IMAGE + ZAUFANIE:** Podpis jest znakiem jakości poczty elektronicznej. Daje on adresatowi pewność, że treść i nadawca są prawdziwi.

## Grupa docelowa

Wszystkie firmy, które chcą wysłać dane wrażliwe pocztą elektroniczną w sposób sprawny i bezpieczny. Wielkość firm waha się od pięciu do wielu tysięcy pracowników / użytkowników.

## Korzyści dla przedsiębiorstw

- Wysyłanie danych wrażliwych standardową pocztą elektroniczną w sposób całkowicie bezpieczny.
- Poufna komunikacja z adresatami na całym świecie - bez potrzeby szczegółowej znajomości infrastruktury mailowej partnera oraz jego urządzeń zabezpieczających.
- Po profesjonalnej implementacji rozwiązanie włącza się płynnie w codzienne procesy pracy i działa praktycznie w sposób niewidoczny.
- Proste, wysoce zautomatyzowane i intuicyjne zarządzanie odciąża dział IT.

## 10 powodów do korzystania z SEPPmail

- Opatentowany proces (GINA) pozwalający komunikować się z każdym adresatem w sposób poufny i prosty. Przy tym nie są konieczne żadne "technologie nośne" jak pdf lub zip, generujące błędy. Potrzebny jest tylko system Mailclient oraz dostęp do internetu z odpowiednią przeglądarką po stronie adresata.
- Zaszifrowane maile i ich załączniki będą wysyłane zawsze w 100%. Dodatkowo zasoby (zapotrzebowanie na miejsce na dysku, kopie zapasowe itp.) nie będą nieustannie rosnąć.
- W przypadku maili GINA można zażądać od adresata potwierdzenia odczytu.
- Portal GINA umożliwia odbiorcy samodzielne zarządzanie swoimi danymi bezpieczeństwa: np. ładuje on swoje klucze publiczne (S/MIME i OpenPGP) we własnym zakresie. Dodatkowo może on sam swoje hasło zmienić lub - w przypadku zapomnienia - zresetować. Może również pobierać klucze od nadawcy, by się z nim bezpieczniej komunikować.
- Załączanie do maili wychodzących różnych standardowych podpisów mailowych (Disclaimer) dla różnych adresów domen. Do maili można przy tym także dodawać podpisy kraju danego adresata.
- Maile GINA są odbierane na wszystkich końcowych urządzeniach mobilnych - BlackBerry 10 i Windows Phone bez ograniczeń; iOS z bezpłatną aplikacją i Android poprzez przeglądarkę Firefox.
- Elegancki, wysoce standaryzowany produkt, dostępny od ręki, z szybką integracją i uruchomieniem.
- Proste zarządzanie za pomocą przejrzyste ułożonych menu i funkcji - np. aktualizowanie do przyszłych wersji za pomocą jednego przycisku, podłączenia Managed PKI (infrastruktury klucza publicznego) do znanych oficjalnych CA (weryfikatorów certyfikatów) lub automatyczne przyporządkowywanie licencji.
- Szyfrowanie Managed Domain i TLS (Transport Layer Security) zawiera się w licencji bazowej. "Managed Domain" oznacza, że urządzenia SEPPmail rozpoznają się na całym świecie i w sposób całkowicie transparentny szyfrują cały ruch maili między skrzynkami pocztowymi SEPPmail.
- Obsługuje szyfrowania:



### **Najlepsze cechy w skrócie:**

- Opatentowana technologia GINA
- Ruleset Engine do realizacji wszystkich specjalnych reguł dotyczących poufnych maili i ich obsługi
- Managed PKI do SwissSign, S-Trust i Sign-Trust
- Clustering zawiera się w licencji bazowej (High Availability i Load Balancing)
- Automatyczne zbieranie certyfikatów S/MIME
- Może obsługiwać kilku klientów
- Portal GINA można dopasować za pomocą kaskadowych arkuszy stylów (CSS) do identyfikacji wizualnej danej firmy
- Wszystkie teksty można dowolnie zmieniać
- Utworzenie własnego disclaimeru
- Aktualizacja za pomocą jednego przycisku
- Szyfrowanie metodą domena-do-domeny zawarte w pakiecie podstawowym.

## **Czy chcesz przetestować to rozwiązanie?**

Pozwól sobie przysłać mail testowy z naszej strony internetowej:

**[www.szyfrowanie-poczty.pl](http://www.szyfrowanie-poczty.pl)**

Poprzez demo online lub skontaktuj się ze mną:

**Jan Zyber**

eSafety Solutions

(+48) 32 32 311 96

[kontakt@szyfrowanie-poczty.pl](mailto:kontakt@szyfrowanie-poczty.pl)