SEPPMAIL
SWISS E-MAIL SECURITY

INFORMACJE O PRODUKCIE

Jan Zyber
eSafety Solutions
(+48) 32 32 311 96
info@esafety-solutions.de

www.szyfrowanie-poczty.pl

SEPPMAIL
SWISS E-MAIL SECURITY

O PRODUKCIE

1) Przy **projektowaniu produktu** postawiono od początku na standaryzację i na to, by powstał produkt nadający się na rynek masowy. Pierwszą wersję zaprezentowano w 2001 roku na rynku szwajcarskim. Odtąd do produktu zasadniczego dodawane są kolejne usprawnienia i rozszerzenia, podczas aktualizacji udostępniane automatycznie wszystkim instalacjom poprzez naciśnięcie przycisku. Skoncentrowano się na powtarzalności i prostocie, a tym samym stabilności.

2) 80-90% wymagań odnośnie zabezpieczonych maili jest realizowane za pomocą ustawień domyślnych. **Ustawienia specjalne, specyficzne dla firm**, można wprowadzać poprzez silny Rulesetgenerator jako narzędzie standardowe. Tym samym możliwe są także projekty bardziej rozbudowane i złożone.

3) Proste i automatyczne działanie: Funkcje takie jak automatyczne zarządzanie kluczami (patrz punkt 4), szyfrowanie domeny (funkcja podstawowa: wszystkie urządzenia SEPPmail rozpoznają się w sieci i szyfrują cały ruch pocztowy w pełni automatycznie - produkty innych firm mogą być podłączane przy pomocy prostej wymiany klucza; bez dodatkowych licencji szyfrowane są wszystkie przychodzące i wychodzące maile między domenami), funkcje portalu (pozwalają użytkownikowi zewnętrznemu bezpiecznie komunikować się z firmą) oraz User Selfservice Password-Management troszczą się o sprawne, proste i ekonomiczne działanie bez dużych kosztów wspierania i ingerencji pomocy technicznej. Kolejną podstawową funkcjonalnością jest wklejanie różnych standardowych podpisów mailowych (Disclaimer) do maili wysyłanych na różne adresy domen. Oznacza to, że można na przykład do maili z adresem hiszpańskim dołączać podpis hiszpański, do maili z aderesem francuskim francuski itd.

4) Managed PKI: oznacza automatyczną integrację oficjalnych CAs. Przy tym SEPPmail samodzielnie wystawia użytkownikowi klucze S/MIME i przedkłada je podłączonemu CA dozezwolenia (CSR). Proces ten przebiega w pełni automatycznie, bez potrzeby ingerencji administratora. Obecnie dostępne są następujące złącza CA: SwissSign, STrust (DSV) i Sign-Trust (Poczta Niemiecka). Oczywiście obsługiwane są także wszystkie inne CAs (np. A/Trust, Comodo), ale te certyfikaty należy wprowadzić w system SEPPmail.

5) Wysoka dostępność jako standardowa funkcjonalność: Clustering i Geoclustering są dostępne jako funkcja podstawowa i konfigurowalne za pomocą kilku kliknięć. Firma GRZ (LOGIS) w Austrii (Raiffeisen Rechenzentrum) prowadzi na przykład jeden Cluster 2x2 SEPPmail w siedzibach w Innsbrucku i Linzu i od 4 lat bez żadnych problemów obsługuje cały ruch mailowy dla 14.000 skrzynek.

6) **Multidomena i możliwość obsługi wielu klientów**: System jest w stanie obsługiwać wielu klientów zarówno dzięki temu, że można tworzyć wiele domen, jak i dzięki temu, że poszczególne zadania administracyjne (zarządzanie relacjami i użytkownikami, Layouting GINA i logowanie) można delegować.

7) Przykładem **akceptacji i rozpowszechnienia** rozwiązania SEPPmail przy jednoczesnej **skalowalności i stabilności** jest www.HIN.ch (Health Information Network) w Szwajcarii. Poprzez to rozwiązanie, bazujące w 100% na SEPPmail, dziennie całą swą komunikację mailową szyfruje 350 szpitali i 17.000 lekarzy (w sumie około 150 tysięcy użytkowników).

Cytat z wypowiedzi administratora w szwajcarskim szpitalu:

> „Dzień dobry!
>
> Zaktualizowałem SEPPMail Gateway do najnowszej wersji Firmware Version 5.3.8. Uważam, że ta aktualizacja jest genialna. Wystarczy nacisnąć przycisk "Aktualizacja" i wszystko działa. Przez 211 dni VM "Uptime" nie sprawiał najmniejszego problemu. Codziennie przychodzi raport, a aktualne listy adresowe system pobiera sobie sam. Także instrukcja HIN jest bardzo dobra: tak dalece przyjazna dla użytkownika, że HIN mógłby prawie zostać filią Apple ;-)"

Również Stowarzyszenie Rolników Szwajcarskich korzysta od roku 2008 z rozwiązania SEPPmail, oraz spotkało się z wysoką akceptacją użytkowników.

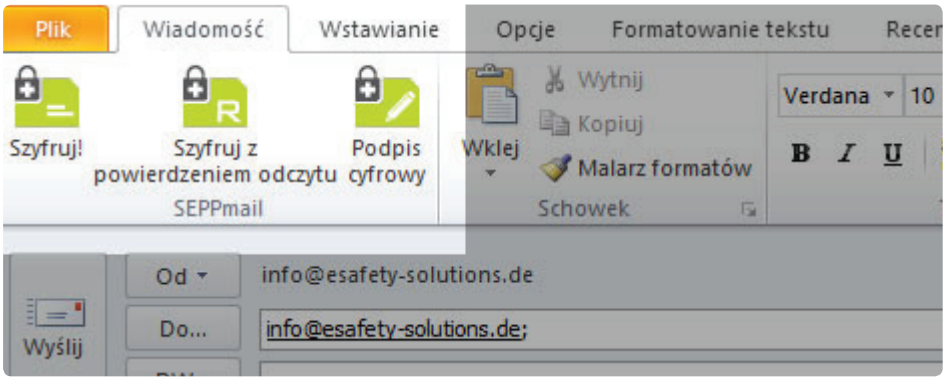
> Doświadczenie wykazuje, że ta aplikacja, prosta i bez niepotrzebnych ozdobników, tak dla nadawcy, jak i dla adresata, ostatecznie osiąga u tychże wysoki poziom akceptacji. Dodatkowe opcje i technologie, takie jak czytnik pdf lub szyfrowanie zip, nie są konieczne, a zatem nie generują całej złożoności i dodatkowych kosztów wsparcia technicznego po stronie użytkownika.

8) **Certyfikaty z przepływu poczty**: Podczas przepływu całego strumienia maili przez urządzenie SEPPmail zbiera ono wszystkie klucze publiczne **S/MIME** cetyfikatów zawartych w podpisach. Certyfikaty S/MIME są – pod warunkiem, że zostały wydane

9) **Adresat nieznany**: Jeśli adresat nie używa żadnego systemu zabezpieczania poczty elektronicznej lub jest całkowicie nieznany, stosuje się naszą **opatentowaną technologię GINA Webmail:** aby adresatowi, którego infrastruktura jest nieznana, przesłać poufnego maila, trzeba mieć tylko jego adres mailowy

Krok 1: Tworzenie i wysyłanie: Nadawca tworzy mail w swoim kliencie poczty. Poprzez kliknięcie na przycisk "Szyfruj", tzw. znacznik w temacie (np. [Poufny]) lub przez reguły ustawione na urządzeniu SEPPmail mail podlega szyfrowaniu, jest dołączany do standardowego maila jako załącznik HTML i wysyłany w ten sposób.

Użytkownikom programu Outlook SEPPmail udostępnia także darmowy plugin:



Mail jest dostarczany całkowicie jako zaszyfrowany załącznik HTML. W wymiarze prawnym powstaje dzięki temu wyraźne przejście do adresata. Ponadto oznacza to ochronę własnych zasobów maszynowych, ponieważ na urządzeniu nie trzeba zapisywać ani przechowywać maili do pobrania. Tym samym nadawca jest zwolniony z obowiązku archiwizowania maili i przechowywania ich przez X lat. Załącznik HTML nie zawiera komponentów aktywnych, dzięki czemu przechodzi przez każdy firewall i jest czytelny w każdej przeglądarce.

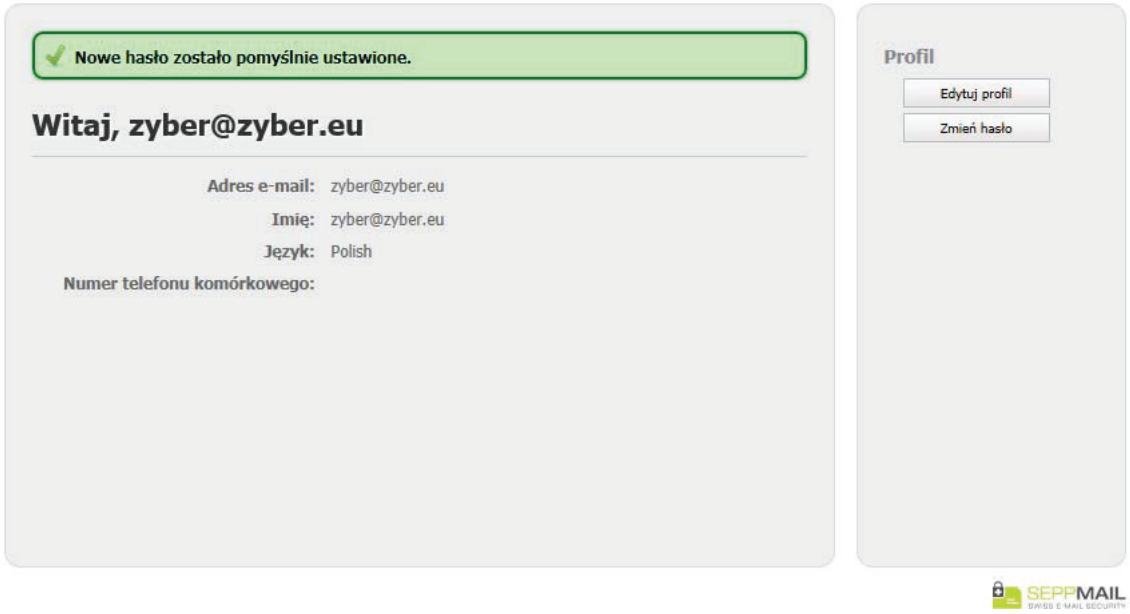
Etap 2: Rejestracja i czytanie. Adresat otwiera załącznik HTML z zaszyfrowaną treścią, podaje swoje hasło i jest jednorazowo prowadzony na stronę logowania.

Tu podaje on swoje indywidualne hasło, zgodne z odpowiednio ustalonymi zasadami i (opcjonalnie) definiuje swoje pytanie bezpieczeństwa z odpowiedzią – na wypadek, gdyby zapomniał hasła (pomoc na rzecz samopomocy).

Jeśli jednak adresat posiada własne klucze (openPGP lub S/MIME), może on załadować go do SEPPmail poprzez portal GINA-Webmail. W przyszłości, co byłoby najkorzystniej, do szyfrowania używany będzie jego aktualny klucz publiczny. Przebyty wcześniej proces uwierzytelniania (2 czynniki: mail + hasło SMS) umożliwi również zaakceptowanie certyfikatów PGP bez dalszego sprawdzania! I to także oznacza oszczędność pracy administratora.

Ten opatentowany proces nie wymaga żadnych dodatkowych warstw technologicznych, takich jak np. konwersja pdf i szyfrowanie zip lub exe. Adresat znajduje swe zasoby poprzez swój standardowy system Mailclient, przeglądarkę i dostęp do internetu.

Ważnym punktem jest **Zarządzanie hasłami**. Na przykład pliki pdf zawsze wymagają hasła przydzielonego w momencie szyfrowania. SEPPmail umożliwia adresatowi w każdej chwili reset i modyfikację hasła. Dlatego adresat przy pierwszym logowaniu ustala także swoje pytanie bezpieczeństwa i odpowiedź.



10) Identyfikację wizualną można w pełni odwzorować za pomocą tzw. CSSs (Corporate Style Sheet). Mailowy interfejs GINA daje się całkowicie dopasować do wymagań biznesowych w zakresie wyglądu. Czcionki, kolory, kształty, przyciski, instrukcje i języki można dowolnie zmieniać. Tym samym możliwa jest także pełna integracja ze stronami internetowymi firmy. Na życzenie wraz z pierwszym mailem może być wyświetlony disclamer, który informuje klienta o jego prawach i obowiązkach, koniecznych do zaakceptowania przy logowaniu.

Przy przyszłych aktualizacjach wszystkie te ustawienia zostaną zachowane

11) Możliwy odbiór na wszystkich urządzeniach mobilnych: zabezpieczone maile GINA można odbierać i czytać na Windows Phone, i-OS, BlackBerry (również BB10) i Android.

12) SEPPmail jest w ofercie zarówno jako **urządzenie sprzętowe**, w 4 klasach wydajności, jak i w wersji wirtualnej maszyny: VM/Image dla ESX (VM-ware), Hyper Visor (RedHat) i Hyper V (Microsoft).

13) SEPPmail: Large File Management (LFM)

Ogólnie znany jest problem odrzucania przez system adresata maili ze zbyt dużymi załącznikami. Funkcjonalność LFM pozwala, by maile od danej ustalonej wielkości były automatycznie przechowywane na urządzeniu w fomie zaszyfrowanej, w celu późniejszego pobrania, i oznaczone "teminem ważności". Adresat otrzymuje mail GINA z wezwaniem do pobrania odłożonego maila w określonym terminie. Pobranie następuje poprzez bezpieczny kanał https. Po upływie terminu ważności plik będzie z urządzenia usuwany. Pliki można dostarczać do urządzenia dwoma drogami: albo klasycznie drogą mailową, albo poprzez standardowo wbudowany portal internetowy. Duże pliki można dostarczać także z zewnątrz, przez portal GINA.

Zalety tego rozwiązania są oczywiste:

- Nadawca może wysyłać bezpośrednio duże pliki.
- Dane są szyfrowane, bez buforowania w chmurze (jak np. w Dropbox).
- Wezwanie do pobrania następuje automatycznie. Adresat może tylko po wyświetlonym terminie ważności rozpoznać, że chodzi o szczególną formę maila GINA, i nie jest obciążany nowym interfejsem, do którego musiałby się przyzwyczaić.
- Rozwiązanie zostało przetestowane przez ekspertów PCI i zaklasyfikowane jako zgodne z wymaganiami!

Rozwiązanie to jest dostępne jako rozszerzenie istniejącego systemu szyfrowania SEPPmail lub jako produkt samodzielny.

SEPPMAIL
SWISS E-MAIL SECURITY

Niektóre funkcje i komponenty:

Komponent	SEPPmail
System bazowy	Specjalnie przygotowane urządzenie ze wszystkimi niezbędnymi komponentami
Aktualizacje	Tylko przez naciśnięcie przycisku, nawet przy aktualizacji systemu operacyjnego
Dostosowania do specyficznych wymagań klienta	Generalnie standaryzowane i włączane do ścieżki rozwoju: Tylko jedna aktualizacja
Instalacja u klienta	Instalacja "od ręki", komponenty zewnętrzne (np. baza danych) nie są konieczne
Zapotrzebowanie na zasoby	Nie ma buforowania maili, dlatego zapotrzebowanie niewielkie
Sprzęt	Sprzęt znormalizowany, ale dostępny także jako VM.
"Mail do osoby trzeciej"	Opatentowany proces GINA jest zarówno łatwy w użyciu, jak i bezpieczny.
Konserwacja	Właściwe porządkowanie nie jest konieczne, ponieważ nie ma rosnącego zapotrzebowania na pamięć
Kopie zapasowe	Pojedyncza kopia zapasowa, dzięki której można odtworzyć cały system
Clustering	Zintegrowana funkcja podstawowa, także dla miejsc oddzielonych w sensie geograficznym
Technologie	S/MIME, openPGP, TLS, GINA (opatentowany webmailer), managed domain key service
Managed PKI	Zautomatyzowane podłączenie SwissSign, S-Trust i Sign-Trust

Czy chcesz przetestować to rozwiązanie?

Pozwól sobie przysłać mail testowy z naszej strony internetowej:

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