SEPPMAIL

SWISS E-MAIL SECURITY

LFM – LARGE FILE MANAGEMENT

SEPPMAIL
SWISS E-MAIL SECURITY

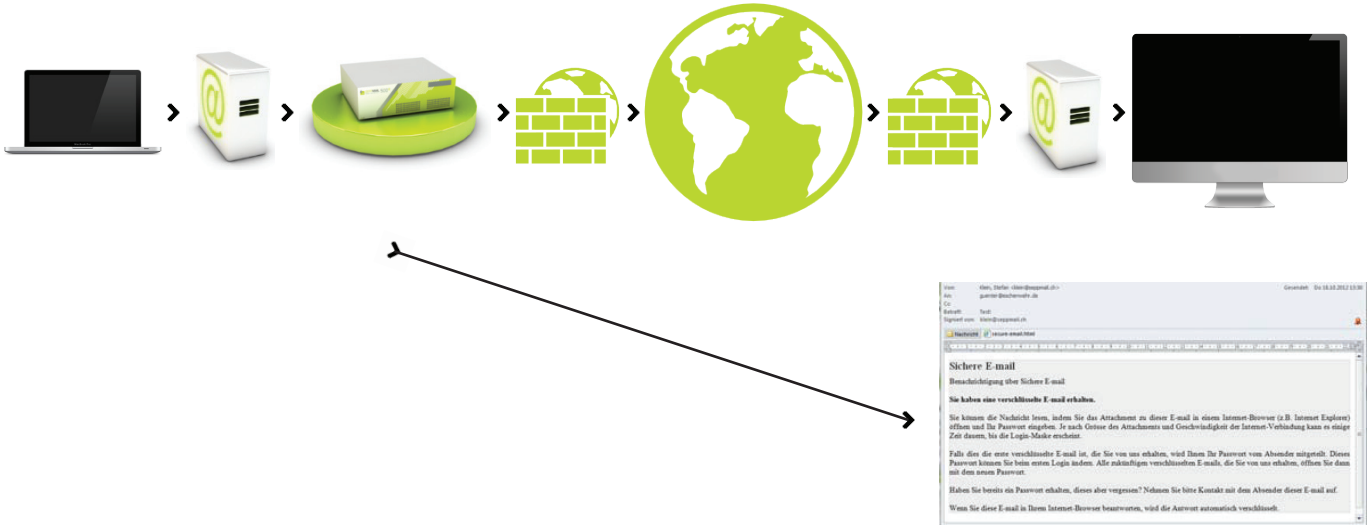
SEPPmail: Large File Management (LFM)

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 bprzyzwyczaić.
- 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.



Mail + załącznik w formie zaszyfrowanej zostaje zatrzymany na urządzeniu, a adresat otrzymuje mailem wezwanie do pobrania.

- Dostarczenie za pośrednictwem sprawdzonej i opatentowanej technologii GINA, automatycznie usuwanie po upływie czasu przechowywania.

- Do ustawienia 3 parametry: rozmiar, czas przechowywania, liczba maili na użytkownika/ dzień.

1) Nadawca tworzy wiadomość + duży załącznik i wysyła je bez dodatkowego oznakowania. SEPPmail rozpoznaje, że wiadomość przekracza ustaloną wartość, i deponuje wiadomość z załącznikami w formie zaszyfrowanej.

2) Adresat otrzymuje mailem wezwanie do odbioru (przy pierwszej komunikacji także hasło wstępne). Proces ten jest identyczny jak przy zaszyfrowanym mailu GINA. Jeśli adresat jest już zarejestrowany, obowiązuje jego już zdeponowane hasło.

3) Mail zawiera załącznik w formacie html + cookies, które ustalają drogę https do urządzenia SEPPmail i animuje GINA-Client do odbioru. Przy odbiorze mail jest na nowo odszyfrowywany na urządzeniu SEPPmail i bezpiecznie dostarczany za pośrednictwem kanału https do adresata.

1) Nadawca tworzy maila + plik w portalu internetowym GINA i dostarcza je bezpośrednio do urządzenia SEPPmail, specjalnie przygotowanego w systemie PCI. W tym urządzeniu mail wraz z załącznikiem jest przechowywany w postaci zaszyfrowanej.

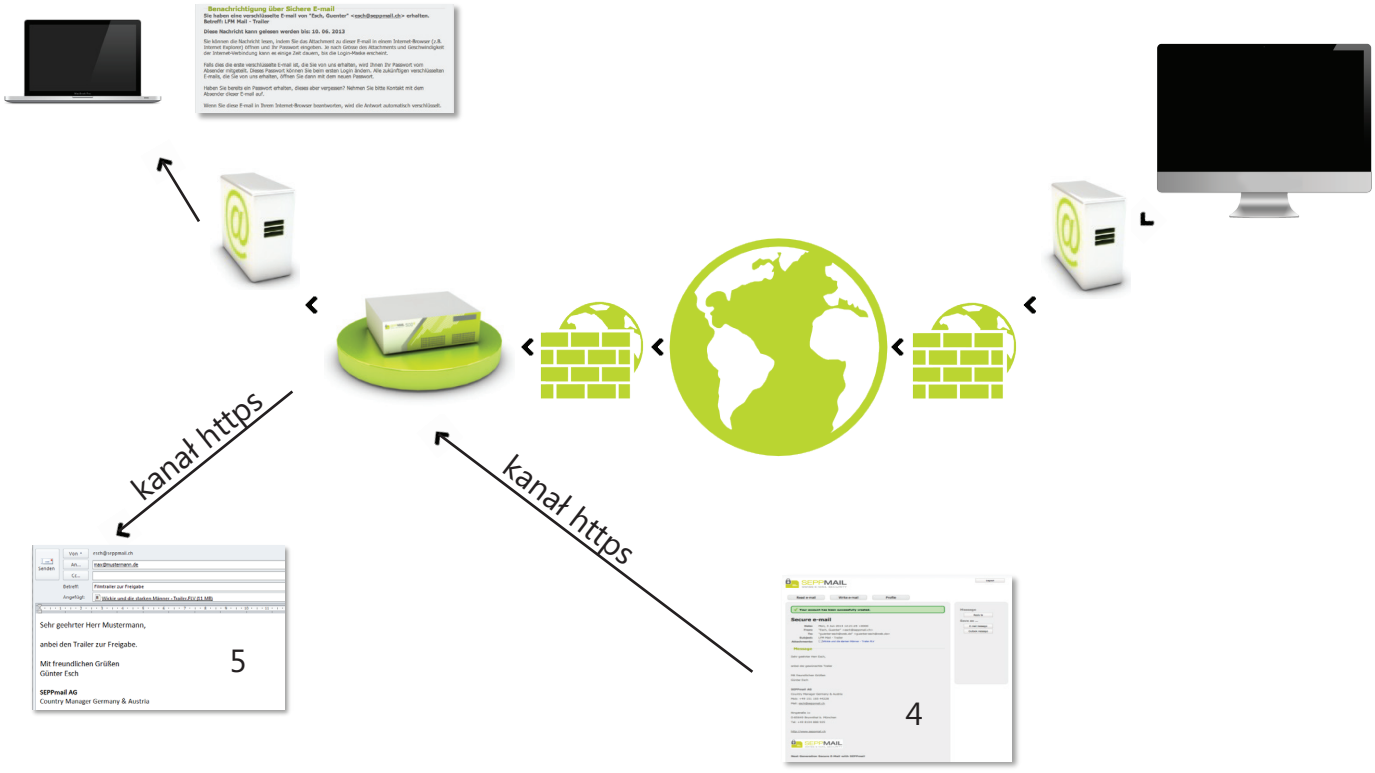
2) Adresat otrzymuje mailem wezwanie do odbioru + przy pierwszej komunikacji także hasło wstępne. Proces ten jest identyczny jak przy zaszyfrowanym mailu GINA.

3) Mail zawiera załącznik html, który ustala drogę https do urządzenia SEPPmail i wzywa klienta GINA do odbioru. Przy odbiorze mail jest na SEPPmail na nowo odszyfrowywany i bezpiecznie dostarczany poprzez kanał https.

Adresat wewnętrzny

Powiadomienie

Nadawca zewnętrzny



4) Nadawca zewnętrzny może również, poprzez otwarty system GINA Client, odstawić mail wraz z załącznikiem do pracownika wewnętrznego bezpieczną drogą https.

5) Także pierwotny nadawca otrzymuje odpowiedź do wewnątrz poprzez system GINA-Client. Przy tym otrzymuje również mailem wezwanie do odbioru.

SEPPMAIL
SWISS E-MAIL SECURITY

Technologie wspieranie przez urządzenie SEPPmail:

Technologie szyfrowania maili, danych i połączeń:

- S/MIME
- PGP
- TLS
- Gateway-to-Gateway
- https (technologia GINA)
- AES 256 (klucz symetryczny)

Funkcje systemowe:

- Może obsługiwać kilku klientów
- Może tworzyć klastry
- Skalowalny (od 5 do ∞ użytkowników)
- Managed PKI (Swisssign; S-Trust; Sign Trust)
- LDAP callforkeys
- Wsparcie dla urządzeń mobilnych (iOS, Android, Windows Phone, BB10)

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