



Problem

Brak możliwości wdrożenia przemysłowego standardu Infrastruktury Klucza Publicznego (PKI) z wykorzystaniem istniejącej w organizacji infrastruktury IBM Lotus Domino/Notes.

Brak możliwości stosowania zewnętrznych kwalifikowanych i bezpiecznych kluczy i podpisów wewnątrz Lotus Domino/Notes.

Brak możliwości kontroli nad informacjami przesyłanymi w wiadomościach zaszyfrowanych za pomocą standardowego mechanizmu Lotus Domino/Notes.

Rozwiązanie – SMI! Encryption Key Manager

Oprogramowanie umożliwiające wdrożenie przemysłowego PKI z wykorzystaniem infrastruktury Lotus Domino/Notes. Korzysta z oprogramowania PEM-HEART, posiadającego deklarację zgodności z Ustawą o podpisie elektronicznym, automatycznie rozpoznającym bezpieczne podpisy weryfikowane przy użyciu kwalifikowanego certyfikatu, a także weryfikującego bezpieczne podpisy zgodnie z logiką określoną w Ustawie.

Razem z SMI! for Domino pozwala kontrolować treść wiadomości zaszyfrowanych w Lotus Domino/Notes, które dotychczas pozostawały poza wszelką kontrolą.

Podstawowe funkcje systemu:

- :: Możliwość szyfrowania, deszyfrowania, podpisywania i weryfikacji podpisu z wykorzystaniem zewnętrznych, kluczy (w tym kluczy kwalifikowanych) x.509 v.3 w środowisku Lotus Notes/Domino.
- :: Możliwość szyfrowania każdego listu i dokumentu dodatkowymi, specjalnymi kluczami: Security Officer i Server, tak aby można było analizować i kontrolować przesyłaną treść przez upoważnioną osobę bądź wyspecjalizowane programy do kontroli treści. O włączeniu lub wyłączeniu tej funkcji decyduje administrator.
- :: Natywna integracja z Lotus Notes i Lotus Domino poprzez mechanizmy rozszerzeń oferowane przez producenta oprogramowania (IBM). Wykluczone jest stosowanie jakichkolwiek utrudnień w korzystaniu aplikacji, typu zmuszenie użytkownika do używania schowka.
- :: Przesyłanie zaszyfrowanej poczty i dokumentów poprzez standardowy protokół Notes Routing.
- :: Szyfrowanie i podpisywanie w locie poczty oraz dokumentów, w tym załączników, bez konieczności wykonywania jakichkolwiek innych czynności poza zaznaczaniem przez użytkownika chęci zaszyfrowania dokumentu bądź jego podpisania.
- :: Korzystanie z podpisów zgodnych ze standardem x.509 zamiast wewnętrznych standardów Lotus Notes/Domino bez blokowania lub z blokowaniem standardowych możliwości Lotus Notes/Domino w tym zakresie. Klucze generowane przez dedykowany zewnętrzny system, bądź otrzymywane z zaufanej jednostki certyfikującej.
- :: Korzystanie z niezależnego od Lotus Domino, zewnętrznego serwera certyfikatów.
- :: Kontrola podpisu podczas otwierania poczty / dokumentu. Sprawdzanie listy unieważnionych podpisów.
- :: Możliwość pracy zarówno z, jak i bez połączenia z centralnym serwerem certyfikatów (praca off-line).
- :: Możliwość korzystania z kluczy przechowywanych: w plikach, na kartach i w zaawansowanych urządzeniach szyfrujących. Administrator ma możliwość wyboru miejsca przechowywania kluczy.
- :: Unieważnianie ważności hasła lub PIN-u do klucza (jeśli klucz wymaga podania hasła lub PIN) po zablokowaniu przez użytkownika stacji Lotus Notes (wylogowanie przez F5).
- :: Podpisy wielokrotne. Znakowanie czasem – automatyczne uwzględnianie odpowiednio kwalifikowanych i niekwalifikowanych znaczników czasu, zależnie od okoliczności.

CHARAKTERYSTYKA

Umożliwia zastosowanie publicznych standardów szyfrujących w infrastrukturze IBM Lotus Domino/Notes.

Pozwala na łatwą implementację kancelarii tajnej.

Umożliwia komunikację z zewnętrznymi instytucjami korzystającymi z podpisów bezpiecznych lub kwalifikowanych.

Uniemożliwia przesyłanie zaszyfrowanych plików i dokumentów zawierających np. treści rasistowskie, ksenofobiczne lub seksualne.

Dedykowany klucz Security Officer umożliwia kontrolę zaszyfrowanych przesyłek pełnomocnikowi ds. bezpieczeństwa.

Dedykowany klucz Servera umożliwia filtrowanie, kontrolę i archiwizację zaszyfrowanych treści.

Pozwala korzystać z kluczy przechowywanych: w plikach, na kartach i w zaawansowanych urządzeniach szyfrujących (DELTA).

Pozwala na kontrolę treści i wyszukiwanie złośliwego oprogramowania (wirusy, trojany itp.) w zaszyfrowanych przesyłkach.

Jest zintegrowany z SMI! for Domino.

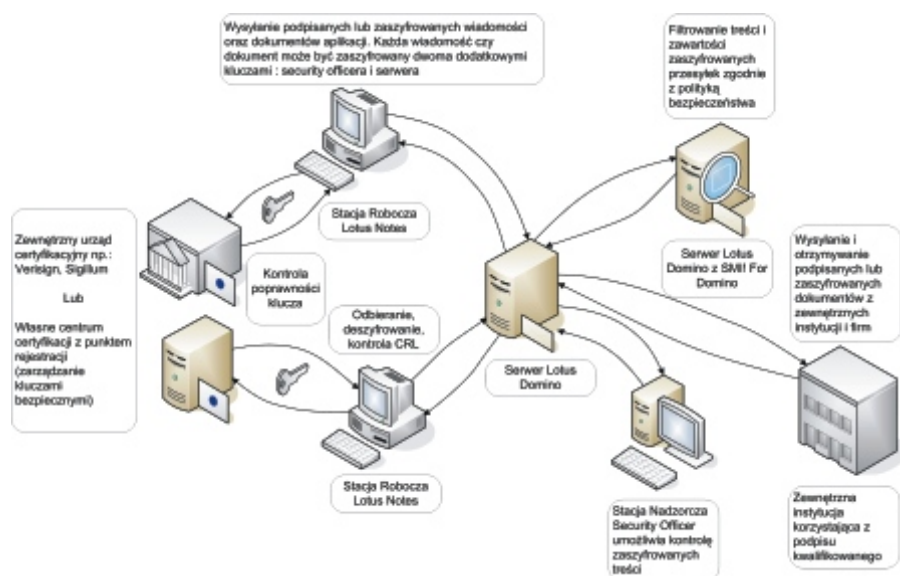
Przez tajemnicę przedsiębiorstwa rozumie się nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Art. 11 ust. 4 Ustawy o zwalczaniu nieuczciwej konkurencji

Jak pracuje SMI! Encryption Key Manager

SMI! Encryption Key Manager został stworzony dla wszystkich użytkowników systemu IBM Lotus Domino/Notes. Praca tego systemu polega na możliwości podmiany standardowych mechanizmów szyfrowania i podpisywania Lotus Notes na klucze zgodne ze standardem x.509 v.3, w tym klucze bezpieczne i kwalifikowane. Dzięki wykorzystaniu oprogramowania PEM-HEART możliwe jest stosowanie zewnętrznych urządzeń szyfrujących.

System SMI! EKM umożliwia zastosowanie zewnętrznych podpisów podczas przesyłania wewnętrznej poczty firmowej oraz we wszystkich istniejących aplikacjach (standardowo Lotus Notes umożliwia wykorzystanie zewnętrznych kluczy tylko w stosunku do poczty wysyłanej poza sieć firmową). Pozwala także na wielokrotne podpisywanie dokumentów elektronicznych, jest to istotne np. we wszelkich systemach obiegu dokumentów, gdzie każda z osób, która zapoznała się z dokumentem powinna go podpisać.



PODSUMOWANIE

Jedyny system umożliwiający wykorzystanie Lotus Domino/Notes do podpisywania i szyfrowania danych z wykorzystaniem zewnętrznych kluczy zarówno w stosunku do poczty zewnętrznej jak i wewnętrznej.

Pozwala na stosowanie skrzynek pocztowych Lotus Domino/Notes do podpisywania i szyfrowania wiadomości bez potrzeby kopiowania lub przenoszenia podpisywanych lub szyfrowanych dokumentów. Podwyższa to komfort pracy oraz zmniejsza ryzyko pomyłki lub utraty danych, a także skraca czas oraz obniża koszty wdrożenia.

Umożliwia wybór sposobu szyfrowania i podpisywania dokumentów. W każdej chwili można wybrać standardowy mechanizm Lotus Domino/Notes lub podpis zgodny ze standardem x.509 v.3.

Dzięki możliwości szyfrowania każdego listu specjalnymi kluczami Security Officer i Server pozwala na kontrolę treści przesyłanych wiadomości oraz zmniejsza ryzyko wycieku poufnych danych, przesyłania i przechowywania zakazanych informacji.

Rodzina produktów Secure Mail Intelligence!®

- :: Secure Mail Intelligence!® for Gateway
- :: Secure Mail Intelligence!® for Domino
- :: Secure Mail Intelligence!® for Exchange
- :: Secure Mail Intelligence!® Managed Service
- :: Secure Mail Intelligence!® Encryption Key Manager

Wymagania techniczne

- IBM Lotus Notes wersja 6.0 lub wyższa (dla stacji roboczej)
- IBM Lotus Domino wersja 6.0 lub wyższa (dla wersji serwerowej)
 - Microsoft Windows 98 lub wyższy (dla stacji roboczej)
 - Microsoft Windows 2000/2003 Server lub nowszy
 - co najmniej 64 MB pamięci RAM
- procesor Pentium III 800 MHz lub szybszy (dla wersji serwerowej)

M2 NET

+48 22 311 18 18, www.m2net.pl