Menedżer kluczy

Menedżera kluczy można używać do tworzenia i zarządzania plikami par kluczy SSL, niezbędnych do ustanawiania szyfrowanych łączy komunikacyjnych z użytkownikami zdalnymi. Oprócz tego Menedżera kluczy można także używać do generowania żądań certyfikatu serwera, który jest plikiem identyfikacji cyfrowej koniecznym do aktywacji pary kluczy SSL. Bez instalacji i przyłączenia ważnego certyfikatu serwera "dołączonego" do pary kluczy nie można korzystać z funkcji zabezpieczeń SSL serwera.

Certyfikat serwera

Certyfikat serwera zawiera informacje identyfikacyjne dotyczące operatora lub organizacji odpowiedzialnej za zawartość witryny sieci Web. Certyfikat serwera zapewnia sposób sprawdzenia przez użytkowników uwierzytelnienia witryny sieci Web i ustanawiania łącza komunikacyjnego z zabezpieczeniem SSL. Certyfikat serwera można otrzymać od cieszącej się powszechnym zaufaniem, niezależnej organizacji, nazywanej *urzędem certyfikacji.* Przed wydaniem ważnego certyfikatu serwera urząd certyfikacji wymaga dostarczenia szczegółowych informacji identyfikacyjnych. Po otrzymaniu pliku certyfikatu można użyć Menedżera kluczy do instalacji certyfikatu serwera.

Para kluczy SSL

Używając Menedżera kluczy tworzy się parę kluczy SSL, która jest niezbędna do ustanowienia łącza komunikacyjnego z zabezpieczeniem. Para kluczy składa się z pliku nazywanego kluczem *publicznym* i kluczem *prywatnym*. Para kluczy jest używana do "negocjacji" bezpiecznego połączenia SSL z przeglądarką sieci Web użytkownika, a nie do szyfrowania przesyłanych informacji.

Utwórz nowy klucz

Należy wpisać informacje do tego okna dialogowego i kliknąć przycisk OK, aby utworzyć dwa pliki. Pierwszy plik jest plikiem kluczy zawierającym parę kluczy. Drugi plik jest plikiem żądania certyfikatu. Kiedy żądanie zostanie przetworzone, usługodawca prześle certyfikat z powrotem do ciebie.

Nazwa klucza Należy przypisać nazwę tworzonemu kluczowi.

Hasło Należy określić hasło, aby zaszyfrować klucz prywatny.

Bity Menedżer kluczy generuje domyślnie parę kluczy o długości 1024 bitów. Aby określić klucz o długości 512 lub 768 bitów, należy dokonać odpowiedniego wyboru w tym polu.

Organizacja Pożądane jest, aby to była organizacja najwyższego poziomu lub nazwa firmy zarejestrowana w International Organization for Standardization (ISO).

Jednostka organizacyjna Oddział firmy, taki jak Marketing.

Przydomek Nazwa domeny serwera, na przykład www.microsoft.com.

Kraj Dwuliterowe oznaczenie kraju, w którym znajduje się siedziba firmy, zgodne z normą ISO, na przykład US, FR, AU, UK itd.

Województwo Należy wpisać pełną nazwę województwa, nie należy stosować skrótów. Na przykład woj. lubelskie, woj. rzeszowskie, woj. wrocławskie itd.

Lokalizacja Należy wpisać pełną nazwę miasta, w którym znajduje się siedziba firmy, taką jak Kraków lub Szczecin.

Plik żądania Należy wpisać nazwę pliku żądania, który będzie utworzony lub zaakceptować nazwę domyślną. Nazwa domyślna jest kopią przypisanej uprzednio nazwy klucza, do której dołączane jest rozszerzenie .req, co razem tworzy nazwę pliku żądania. Jeśli na przykład w polu **Nazwa klucza** zostało wpisane słowo "zabezpieczenie", domyślna nazwa pliku żądania będzie miała postać zabezpieczenie.req.

Notka

W żadnym polu nie wolno używać przecinków. Przecinki są interpretowane jako koniec tego pola i będą generować nieprawidłowe żądania bez ostrzeżenia.

Po wpisaniu wszystkich informacji należy kliknąć przycisk OK. Kiedy pojawi się żądanie, należy ponownie wpisać swe hasło, a następnie kliknąć przycisk OK. Nazwa utworzonego klucza pojawi się w oknie Menedżera kluczy poniżej nazwy komputera.

Tworzenie kopii zapasowych plików par kluczy SSL

Pary kluczy SSL są niezbędne do zapewnienia bezpieczeństwa szyfrowanej komunikacji. Pary kluczy związane z ważnym certyfikatem serwera zapewniają wysoce niezawodną i unikatową identyfikację witryn sieci Web. Osoba nie upoważniona mająca dostęp do twojej pary kluczy może poważnie zagrozić bezpieczeństwu komunikacji i transakcji.

Ze względu na znaczenie pary kluczy SSL dla zabezpieczenia, a w niektórych wypadkach, ze względu na koszty związane z uzyskaniem ważnego certyfikatu serwera, należy podjąć wszelkie wysiłki, aby chronić parę kluczy przed przypadkową stratą lub kradzieżą.

Aby sporządzić kopię zapasową pary kluczy SSL

1. Wybierz klucz.
2. W menu **Klucz** zaznacz polecenie **Eksportuj klucz**, a następnie kliknij przycisk **Plik kopii zapasowej**.
3. W ostrzegawczym oknie dialogowym **Menedżera kluczy** przeczytaj komunikat ostrzegawczy, a następnie kliknij przycisk **OK**.
4. Zapisz plik pary plików używając rozszerzenia .txt.

Notka

Plik pary kluczy należy zapisać w katalogu zabezpieczonym odpowiednimi uprawnieniami systemu plików Windows NT (NTFS), które ograniczają nieupoważniony dostęp, albo na dysku, który będzie przechowywany w bezpiecznym miejscu.

Wybierz adres IP

Należy wybrać adres Internet Protocol (IP) serwera, do którego ma być zastosowany klucz warstwy Secure Sockets Layer albo wpisać adres IP.

Podłącz do komputera

To okno dialogowe umożliwia utworzenie pliku żądania klucza i pary kluczy dla serwera zdalnego.

Komputer Należy wpisać nazwę komputera serwera, z którym chcesz się połączyć.

Jak uzyskać certyfikat

Aby dowiedzieć się, jak można uzyskać certyfikat VeriSign, należy się połączyć z witryną VeriSign usługi Web, www.verisign.com.

Łączy się z określonym serwerem.

Rozłącza się od określonego serwera.

Zmiany rekordów klucza na określonym serwerze.

Tworzy nowy klucz.

Ponawia poprzednie żądanie certyfikatu klucza.

Instaluje nowy klucz po odebraniu certyfikatu.

Usuwa wybrany klucz.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.

Pomoc do tego tematu nie jest dostępna.