Dokumentacja programu Kryptograf

Wersja 1.0.x

Top-Team TT Sp. z o.o.

www.top-team.pl

Spis treści

Rozdział 1. O programie

Kryptograf jest programem służącym do składania lub weryfikacji podpisu elektronicznego.

1.1. Środowisko

Program działa na platformach Windows i Linux. Obsługuje się go przez dowolną przeglądarkę internetową.

1.2. Wymagania

Do poprawnego działania programu wymagane są Java 8 i Tomcat 8.

Rozdział 2. Uwagi wstępne

Ważne

Kryptografa instaluje się na komputerach Użytkowników korzystających ze sprzętowego podpisu elektronicznego. Instalacja na serwerze, na którym zainstalowane są aplikacje dziedzinowe Top-Team, nie jest wymagana (poza przypadkiem, gdy serwer jest jednocześnie komputerem Użytkownika).

Ponieważ Kryptograf jest aplikacją webową, wymaga tego samego, co reszta programów Top-Team, środowiska uruchomieniowego. Następny rozdział zawiera wskazówki dotyczące instalacji Javy, Tomcata i TT-Managera.

Rozdział 3. Przygotowania

3.1. Instalacja Javy

Instalację Javy należy przeprowadzić wg instrukcji zawartych w dokumentacji TT-Managera.

-> Rozdział 2.1. Instalacja Javy [https://top-team.pl/pub/docs/tt_manager/przygotowania.html#przygotowania_java]

3.2. Instalacja Tomcata

Instalację Tomcata należy przeprowadzić wg instrukcji zawartych w dokumentacji TT-Managera.

-> Rozdział 2.2. Instalacja Tomcata [https://top-team.pl/pub/docs/tt_manager/przygotowania_tomcat.html]

3.3. Instalacja TT-Managera

Instalację TT-Managera należy przeprowadzić wg instrukcji zawartych w dokumentacji TT-Managera.

-> Rozdział 3. Instalacja (TT-Managera) [https://top-team.pl/pub/docs/tt_manager/instalacja.html]

Rozdział 4. Instalacja

Ważne

Kryptografa instaluje się na komputerach Użytkowników korzystających ze sprzętowego podpisu elektronicznego.

Instalację Kryptografa należy przeprowadzić wg instrukcji zawartych w dokumentacji TT-Managera.

-> Rozdział 3. Instalacja (aplikacji) [https://top-team.pl/pub/docs/tt_manager/obsluga_aplikacje.html#d5e276]

Podpowiedź

- Aplikacja, którą należy wybrać, to oczywiście "kryptograf".
- Najodpowiedniejszy w większości przypadków będzie kanał "stable".
- Zainstalowanie najnowszej wersji osiąga się pozostawiając pole wersji puste.
- Domyślną, a jednocześnie zalecaną ścieżką instalacji jest "/kryptograf".

Rozdział 5. Konfiguracja

Aby wyświetlić konfigurację Kryptografa, należy postąpić wg instrukcji zawartych w dokumentacji TT-Managera.

-> 4.2.3. Konfiguracja (aplikacji) [https://top-team.pl/pub/docs/tt_manager/obsluga_aplikacje.html#d5e337]

5.1. Zawartość

Aplikacje :: /kryptograf.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
    <comment>Kryptograf</comment>

    <!-- ustawienia PKCS11 -->
    <entry key="pkcs11.libraries">moja_biblioteka_pkcs11</entry>

</properties>
```

Rysunek 5.1. Przykładowa zawartość konfiguracji

Wpis "pkcs11.libraries" powinien zawierać skróconą (pozbawioną rozszerzenia) nazwę lub pełną ścieżkę do bilioteki implementującej interfejs PKCS11. W zależności od systemu operacyjnego, będzie to plik .dll (Windows) lub .so (Linuks).

Podpowiedź

Bibliotekę można najczęściej znaleźć w katalogu systemowym (można wtedy użyć nazwy skróconej), ewentualnie w katalogu oprogramowania dostarczanego przez producenta podpisu (konieczne jest podanie pełnej ścieżki).

Przykładowe wartości "pkcs11.libraries" zawiera następny podrozdział.

5.2. Przykłady

Poniższa lista zawiera przykładowe wartości wpisu "pkcs11.libraries".

- Asseco Poland S.A.
  - cryptoCertum3PKCS
  - SimplySignPKCS
  - C:\Windows\System32\cryptoCertum3PKCS.dll
  - C:\Windows\System32\SimplySignPKCS.dll
  - C:\Program Files\Certum\SimplySign Desktop\proCertum SmartSign\cryptoCertum3PKCS.dll
- Centrum Certyfikacji Kluczy CenCert (Enigma Systemy Ochrony Informacji Sp z o.o.)
  - enigmap11
  - C:\Windows\System32\enigmap11.dll
  - C:\Program Files\ENCARD\enigmap11-x64.dll
- CryptoTech Sp. z o.o.
  - CCPkiP11
  - C:\Windows\System32\CCPkiP11.dll
  - C:\Program Files\CryptoTech\CryptoCard\CCP1164.dll
  - C:\Program Files (x86)\CryptoTech\CryptoCard\CCPkiP11.dll
- EuroCert Sp. z o.o.
  - cmp11
  - C:\Windows\System32\cmp11.dll
- KIR (Krajowa Izba Rozliczeniowa S.A.)
  - CCP11s

  - CCP1164
  - CCPkiP11
  - Graphitep11
  - Graphitep1164
  - C:\Windows\System32\CCP11s.dll
  - C:\Program Files\CryptoTech\CryptoCard\CCP1164.dll
  - C:\Program Files (x86)\CryptoTech\CryptoCard\CCPkiP11.dll
  - C:\Program Files (x86)\Krajowa Izba Rozliczeniowa S.A\CCAktywator\Graphitep11.dll
  - C:\Program Files (x86)\Krajowa Izba Rozliczeniowa S.A\CCAktywator\Graphitep1164.dll
- Sigillum (PWPW Technologie IT)
  - asepkcs
  - CCPkiP11
  - C:\Windows\System32\CCPkiP11.dll
  - C:\Program Files (x86)\CryptoTech\CryptoCard\CCPkiP11.dll

Podpowiedź

Preferowane jest użycie skróconej nazwy biblioteki (np. "pkcs11"). Pełną ścieżkę (np. "C:\Windows\System32\pkcs11.dll") należy podać dopiero wtedy, gdy skrócona nazwa nie zostanie rozpoznana.

Podpowiedź

Możliwe jest skonfigurowanie kilku podpisów dostarczanych przez różnych producentów. Odpowiadające im wartości wpisu "pkcs11.libraries" należy wtedy oddzielić średnikami.

5.3. Zabezpieczenia

Zaleca się tak skonfigurować serwer Apache Tomcat, aby komunikacja odbywała się z użyciem protokołu HTTPS.

Ostrzeżenie

Komunikacja przeprowadzana bez użycia szyfrowania może skutkować dostaniem się numeru PIN w niepowołane ręce.

Pełna dokumentacja konfiguracji SSL/TLS dostępna jest na stronie Apache Tomcat 8 w dziale SSL/TLS Configuration: https://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html

5.4. Weryfikacja

Konfigurację można zweryfikować odwiedzając adresy wskazane w kolejnych sekcjach.

Podpowiedź

Adresy mogą się różnić, jeśli Tomcat skonfigurowano na portach innych niż 8080 / 8443.

5.4.1. Usługi PKCS11

Stan usług kryptograficznych dotyczących sprzętowych podpisów elektronicznych można zweryfikować odwiedzając jeden z poniższych adresów.

- http://localhost:8080/kryptograf/pkcs11/certyfikaty (połączenie nieszyfrowane)
- https://localhost:8443/kryptograf/pkcs11/certyfikaty (połączenie szyfrowane)

Rozdział 6. Licencje

This product includes software developed by IAIK of Graz University of Technology.

6.1. IAIK PKCS#11

IAIK PKCS#11 Wrapper License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by IAIK of Graz University of Technology."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Graz University of Technology" and "IAIK of Graz University of Technology" must not be used to endorse or promote products derived from this software without prior written permission.

5. Products derived from this software may not be called "IAIK PKCS Wrapper", nor may "IAIK" appear in their name, without prior written permission of Graz University of Technology.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE LICENSOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.