Elektroniczny notariat Stemplowanie czasem

Autor:
Paweł Marszałek

Kierujący pracą:
prof. dr hab. inż. Zbigniew Kotulski

Plan prezentacji

- Co to jest stemplowanie czasem?
- Istniejące rozwiązania
- Moja aplikacja - założenia
- Opis algorytmu - RFC3161
- Serwery czasu jako TSA - wymagania
- Wiarygodność TSA

Co to jest stemplowanie czasem?

- Dokument nie został zmieniony po określonym czasie
- Pewna data
- Wykorzystywane w podpisie elektronicznym

Kwestie prawne

Art. 7 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (DzU 2001 Nr 130, poz. 1450) -

„Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów kodeksu cywilnego”

W Unii Europejskiej pierwsze zapisy dotyczące znakowania czasem pojawiły się w dyrektywie 1999/93/EC z 13 grudnia 1999 r., gdzie wspomniano, iż usługi związane z podpisem elektronicznym powinny obejmować znakowanie czasem.

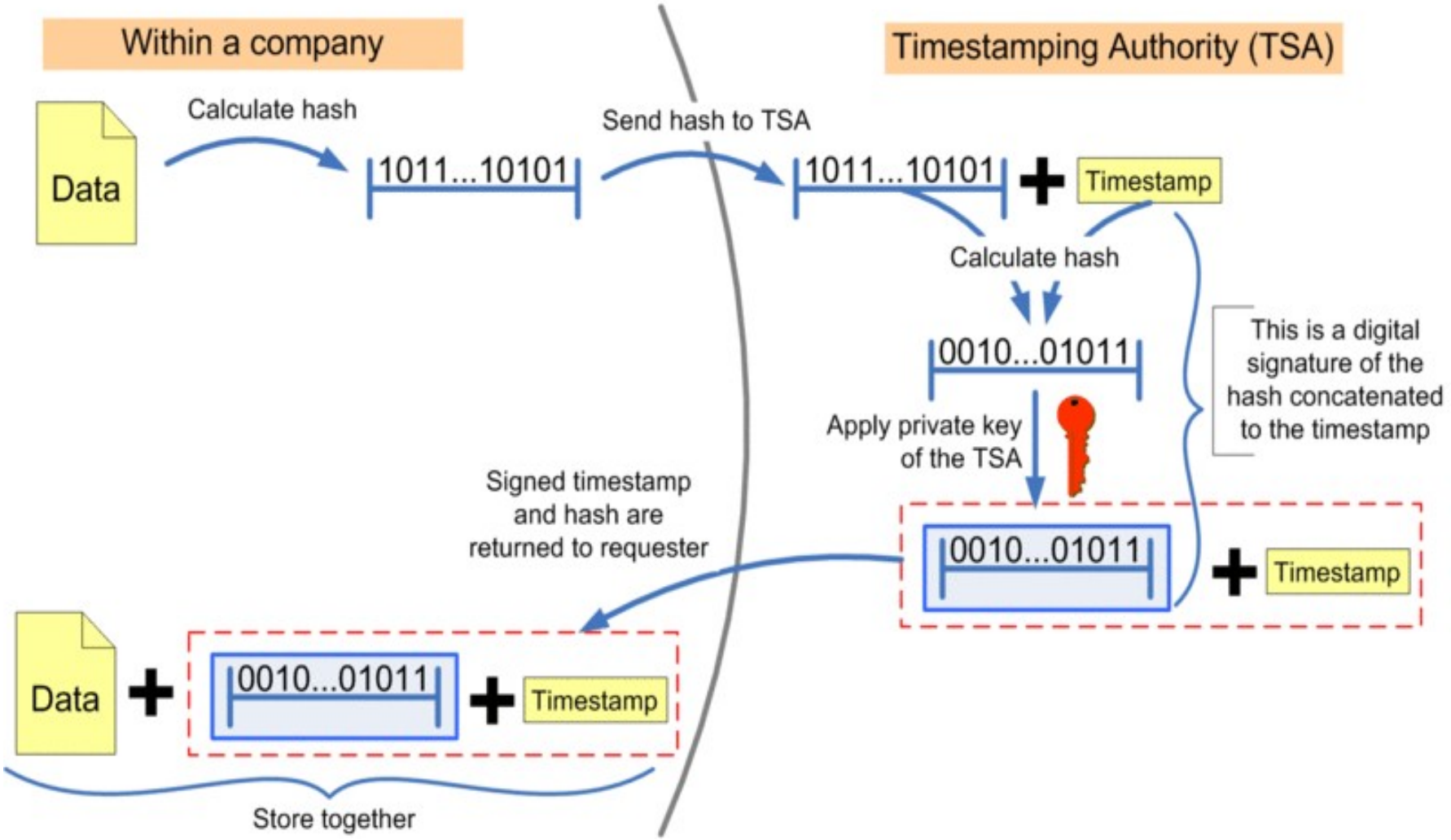
Istniejące rozwiązania

- Centrum Certyfikacji Signet [www.signet.pl]
- Polskie Centrum Certyfikacji Elektronicznej Sigillum [www.sigillum.pl]
- Centrum Certyfikacji Unizeto CERTUM [www.certum.pl]

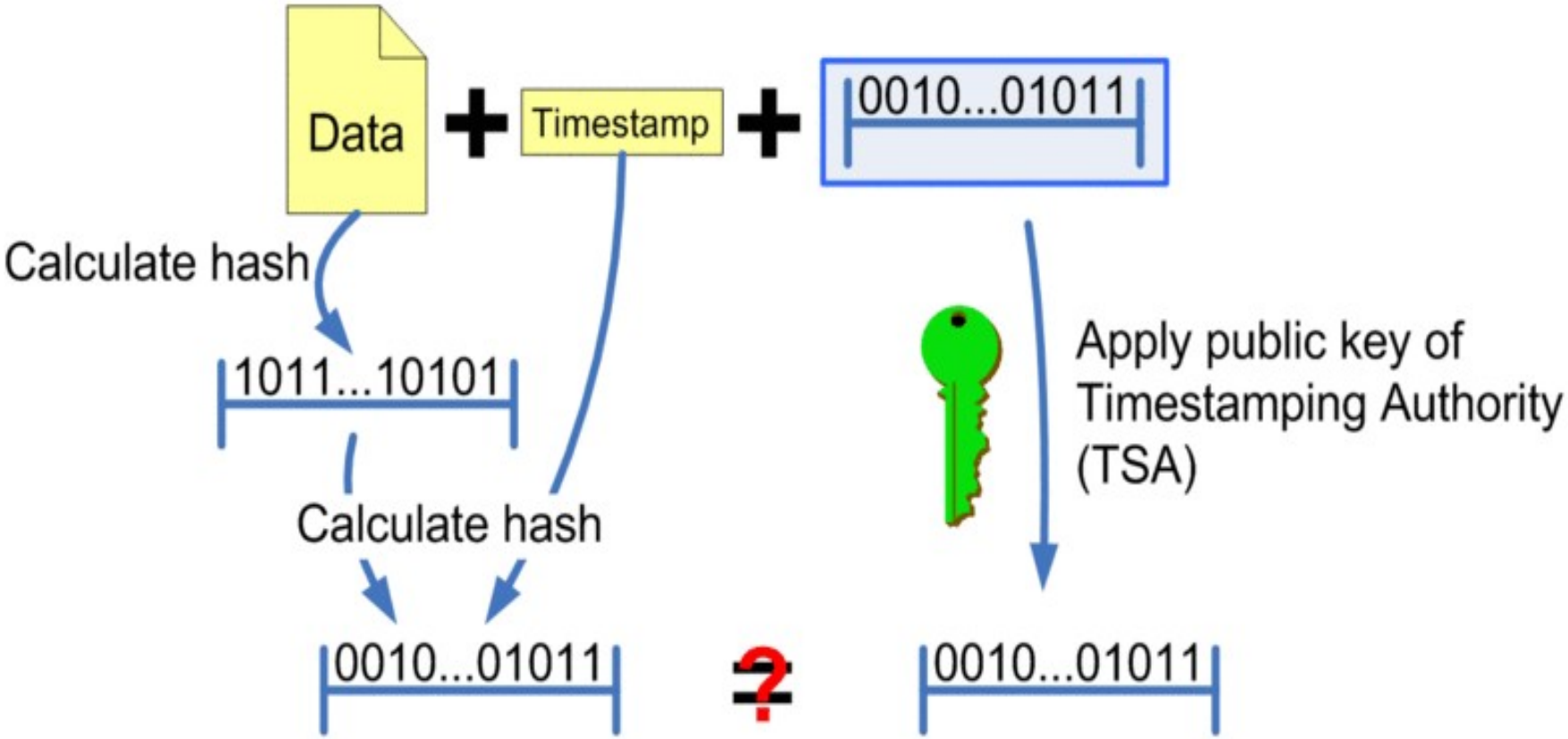
Moja aplikacja - założenia

- Aplikacja desktopowa
- Język – JAVA
- Stemplowanie czasem i weryfikacja
- Wykorzystanie publicznych serwerów czasu jako TSA
- Protokół HTTP

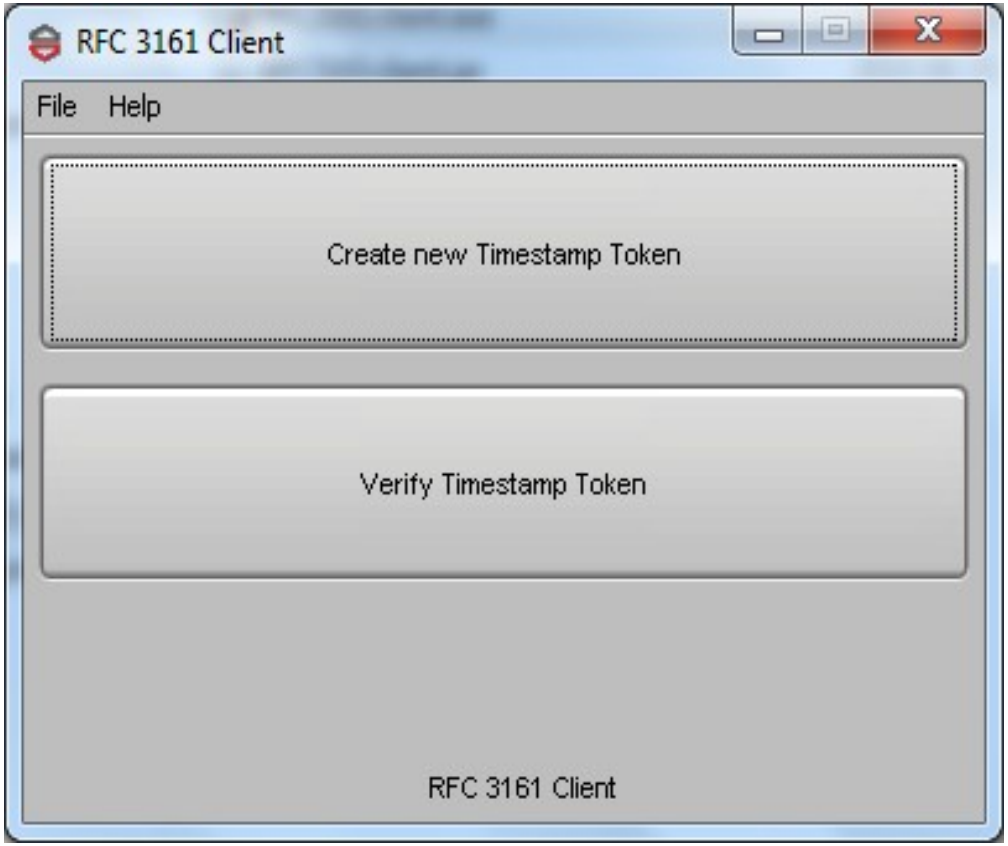
Trusted timestamping



Checking the trusted timestamp



Klient


RFC 3161 Client
File
Help
Create new Timestamp Token
Verify Timestamp Token
RFC 3161 Client

TSA


ELPROMA
exact time
GPS Network Time Server
NTS-5000
Powered by Rubidium & OCXO
Setup Keyboard
Status Display

RFC3161

- Funkcja skrótu: SHA-1, MD-5, RIPEMD-160
- Protokół: HTTP, e-mail
- Każdy token posiada inny numer
- Archiwizacja tokenów
- Rożne klucze do różnej polityki

Wymagania względem TSA

- TSA musi korzystać z usług wiarygodnego dostawcy czasu
- Każdy dokument, który uzyskał stempel czasu musi posiadać swój unikalny identyfikator
- TSA musi zapisać w żetonie czasu technikę wykorzystaną do jego utworzenia
- Żetony czasu nie mogą umożliwiać uzyskania informacji na temat klienta centrum autoryzacji osobom niepowołanym

Serwery czasu jako TSA

- Protokół NTP
- Synchronizacja do sygnału GPS
- Oscylator cezowy
- Inne serwery

Wiarygodna skala czasu

- Kilka serwerów w jednej sieci odpowiedzialnej za czas
- Protokół NTP i falseticker

Certyfikaty, klucze...

- Ważność certyfikatu
- Wymiana kluczy
- Przechowywanie kluczy

Literatura

- *RFC3161*
- *FIPS1401*
- *RFC2630*
- *Mills, David: Computer Network Time Synchronization: the Network Time Protocol*
- *Masashi Une: The Security Evaluation of Time Stamping Schemes*

Dziękuję za uwagę

Zapraszam do dyskusji...