Politechnika Poznańska
Wydział Elektryczny
Instytut Automatyki i Inżynierii Informatycznej

Baza danych dokumentów podpisanych stemplami czasowymi

Autorzy:
Maciej Marciniak
nr indeksu: 121996
e mail:
maciej.r.marcniak@student.put.poznan.pl

Damian Filipowicz
nr indeksu: 122002
e mail:
Damian.Filipowicz@student.put.poznan.pl

Krzysztof Łuczak
nr indeksu: 122008
e mail:
krzysztof.t.luczak@student.put.poznan.pl

Dawid Wiktorski
nr indeksu: 122056
e mail:
dawid.wiktorski@student.put.poznan.pl

25 kwietnia 2017

Spis treści

Rozdział 1

Ogólny opis systemu

System ten będzie służyć do uzyskiwania podpisów cyfrowych ze stemplem czasowym, który będzie wiarygodny poprzez zastosowanie urzędu certyfikacyjnego w postaci serwera połączonego z bazą danych. Użytkownik przy pomocy aplikacji lub strony internetowej będzie przesyłał dokument wraz z funkcją skrótu, następnie serwer będzie swoim własnym podpisem dawał stempel czasowy, który będzie umieszczał w bazie danych i odsyłał użytkownikowi (do aplikacji lub strony WWW) dokument wraz z podpisem cyfrowym zawierającym stempel czasowy. Dzięki temu dokumenty będą miały wiarygodny stempel czasowy pozwalający określić dokładną godzinę zatwierdzenia dokumentu w systemie autentykacji.

W skład systemu będzie wchodzić:

- aplikacja serwerowa z bazą danych,
- aplikacja webowa,
- aplikacja mobilna,
- aplikacja desktopowa.

Rozdział 2

Organizacja pracy

2.1 Podział zadań

Realizacja projektu odbywać się będzie w modułach tworzonych współbieżnie:

- dokumentowania projektu,
- tworzenia aplikacji serwerowej,
- tworzenia aplikacji webowej,
- tworzenia aplikacji mobilnej,
- tworzenia aplikacji desktopowej,
- mechanizm uwierzytelniania.

Wyszczególniony podział modułów pomiędzy członków zespołu przedstawiony został w Tabeli 2.1.

Tabela 2.1: Podział zadań projektowych

Osoba	Rola
Maciej Marciniak	Kierownik, programista: dokumentacja, organizacja zespołu, aplikacja serwerowa
Dawid Wiktorski	Programista: aplikacja mobilna na system Android, aplikacja serwerowa
Krzysztof Łuczak	Programista: aplikacja webowa, aplikacja serwerowa, mechanizm uwierzytelniania
Damian Filipowicz	Programista, aplikacja desktopowa, aplikacja serwerowa

2.2 Harmonogram pracy

Harmonogram pracy zespołu przedstawiony został na wykresie Gantta, który znajduje się w linku poniżej do arkusza Google: Harmonogram prac

2.3 Repozytiorium GitHub

Repozytorium GitHub

Rozdział 3

Schemat idei stempli czasowych

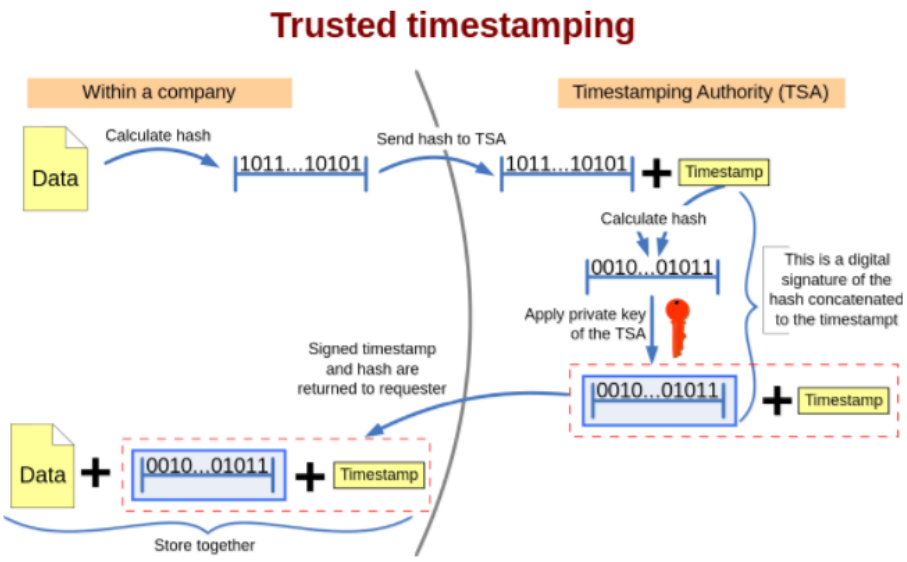
Na dokument podpisany stemplem czasowym składają się trzy pliki:

- podpisywany dokument,
- stempel czasowy,
- wygenerowany certyfikat uwierzytelniający stempel czasowy.

Tworzenie dokumentu podpisanego stemplem czasowym

Tworzenie certyfikatu odbywa się po stronie zaufanego urzędu poprzez dodanie do funkcji skrótu podpisywanego dokumentu, stempla czasowego, a następnie z utworzonej paczki ponownie tworzy się funkcję skrótu. Ostatecznie skrót obu plików szyfruje się kluczem prywatnym i przesyła się z powrotem do użytkownika.

Schemat przebiegu tworzenia dokumentu przedstawiony jest na Rysunku 3.1.

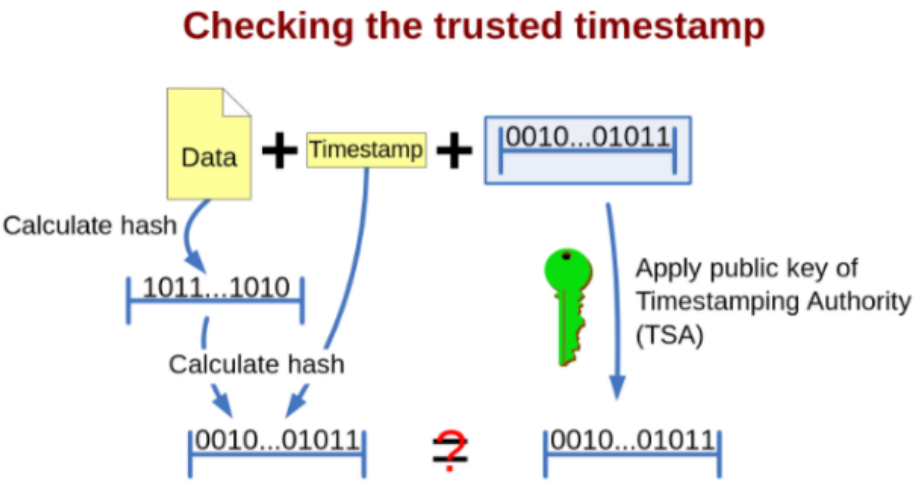


Rysunek 3.1: Diagram tworzenia stempli czasowych

Weryfikacja dokumentu podpisanego stemplem czasowym

Weryfikacja certyfikatu odbywa się po stronie użytkownika poprzez wykonanie funkcji skrótu dokumentu, następnie dodanie do niej dołączonego stempla czasowego i ponowne wykonanie funkcji skrótu. Certyfikat należy odszyfrować kluczem publicznym użytkownika, po czym porównać utworzone ciągi znaków. Jeżeli otrzymane pliki są identyczne, to dokument został podpisany o podanej godzinie, która umieszczona jest w dołączonym pliku stempla czasowego.

Schemat przebiegu weryfikacji dokumentu przedstawiony jest na Obrazie 3.2.

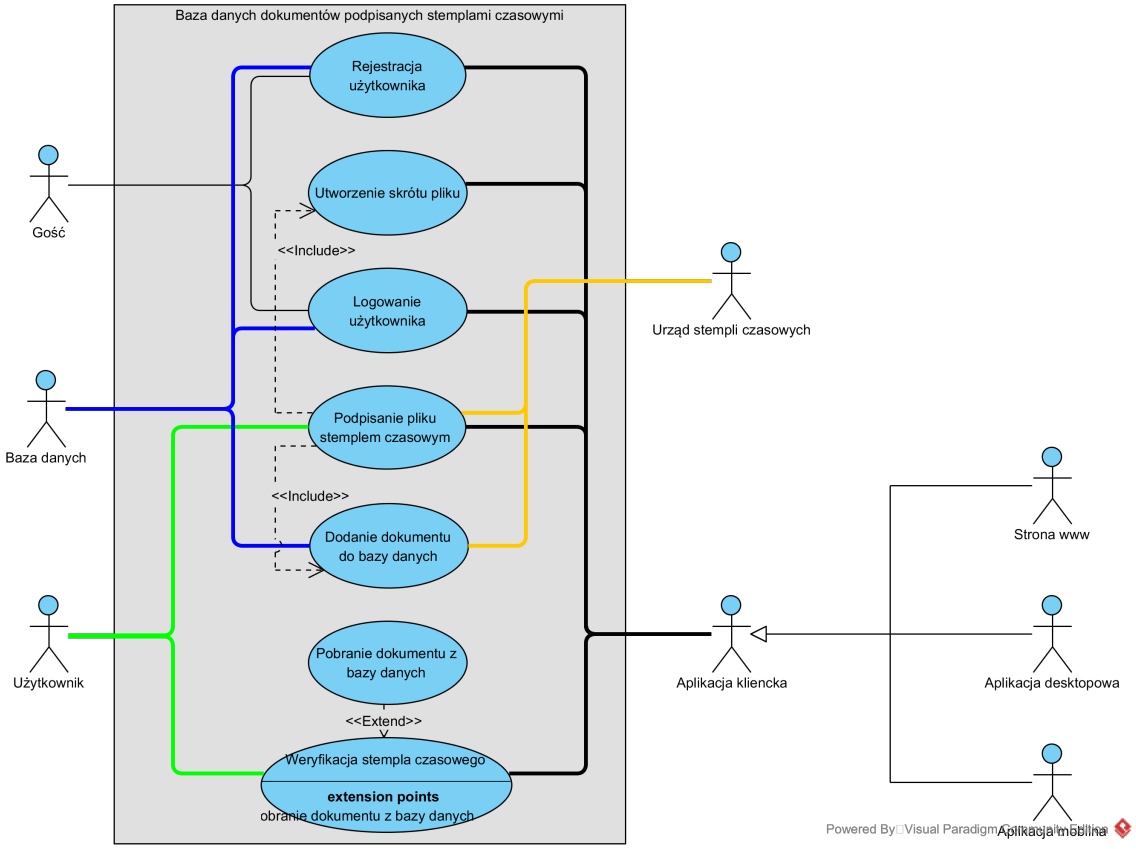


Rysunek 3.2: Diagram weryfikacja stempli czasowych

Rozdział 4

Diagramy UML systemu

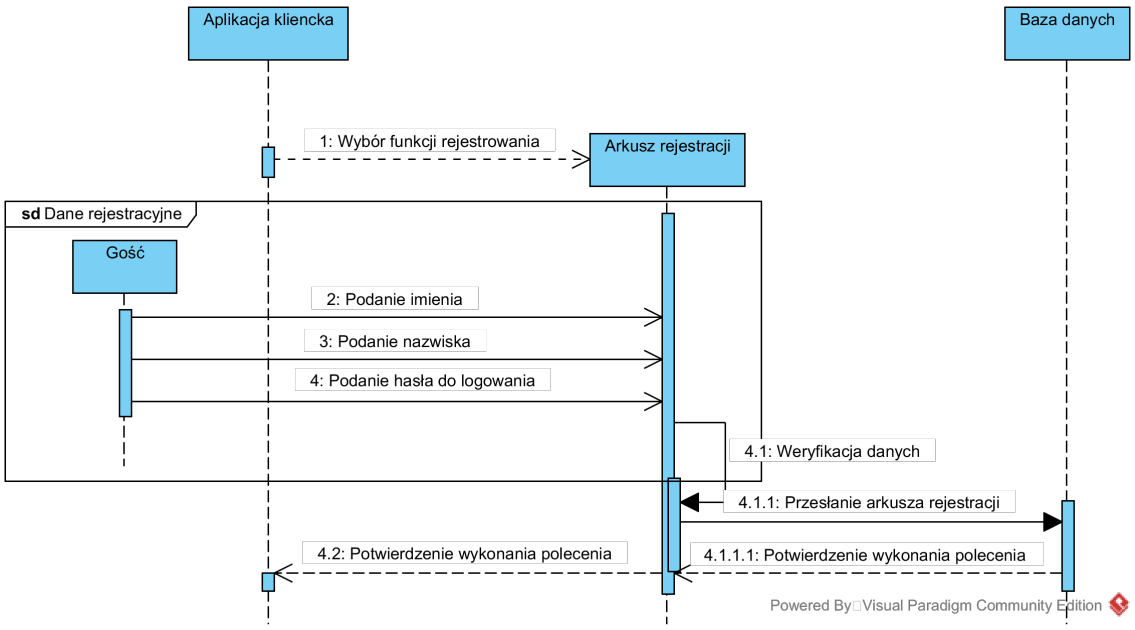
4.1 Diagram przypadków użycia



Rysunek 4.1: Diagram przypadków użycia

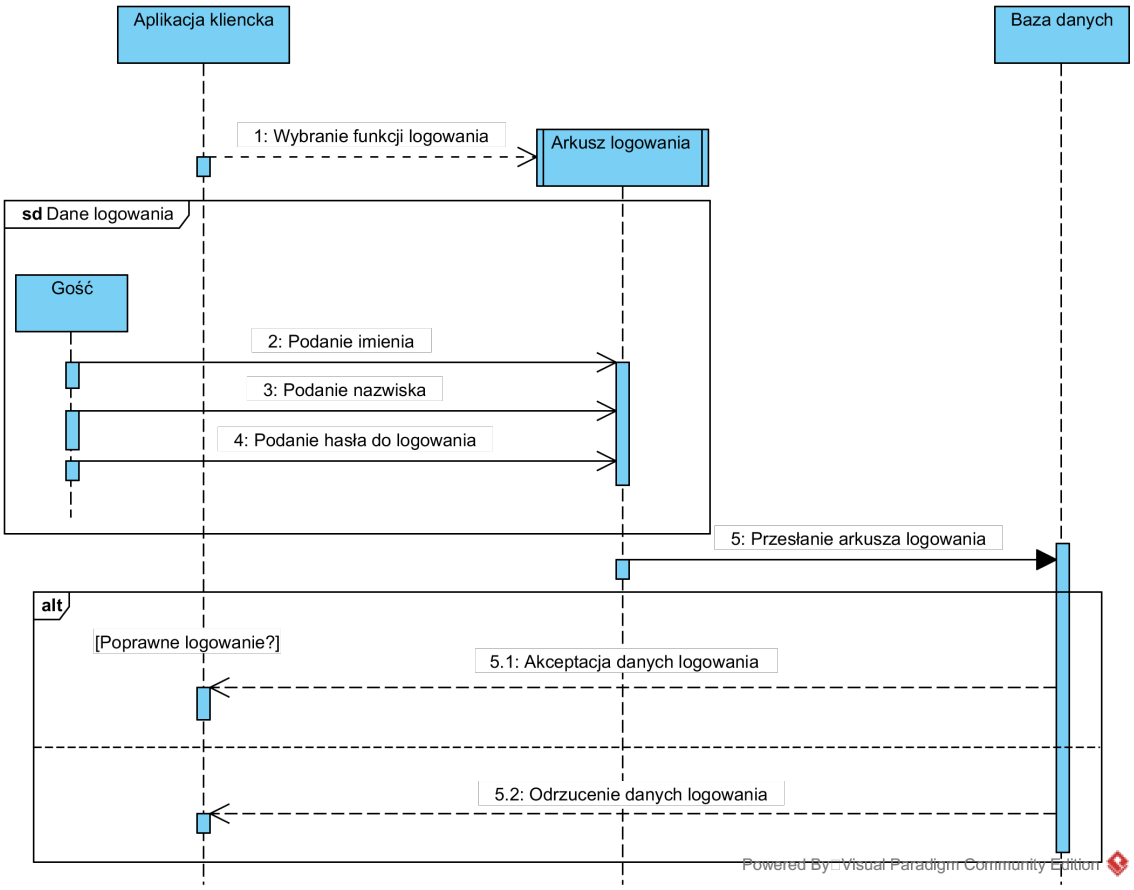
4.2 Diagramy sekwencji

Rejestracja użytkownika



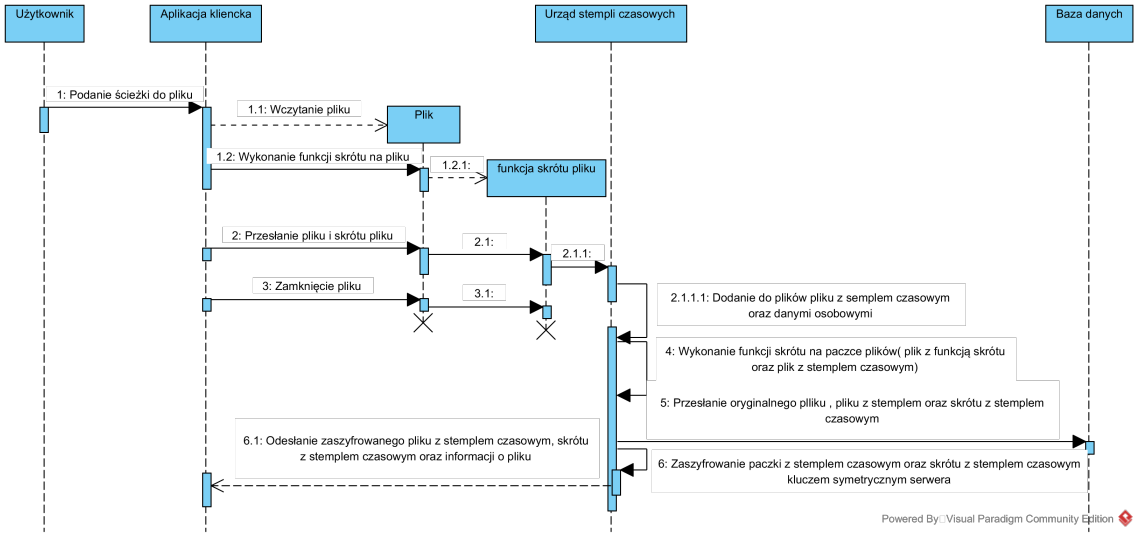
Rysunek 4.2: Diagram sekwencji rejestracji użytkownika

Logowanie użytkownika



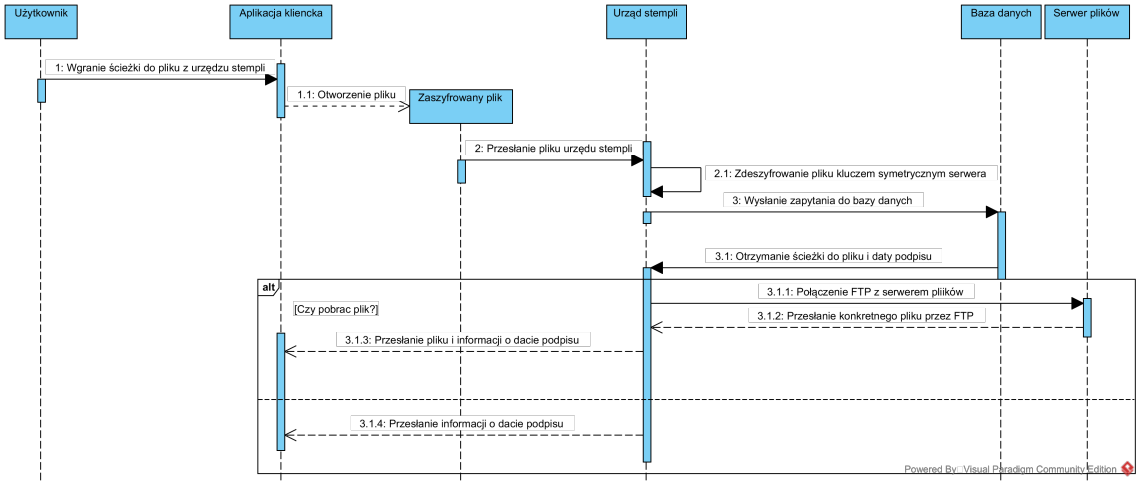
Rysunek 4.3: Diagram sekwencji logowanie użytkownika

Podpis pliku stemplem czasowym



Rysunek 4.4: Diagram sekwencji podpisu pliku stemplem czasowym

Weryfikacja stempla czasowego



Rysunek 4.5: Diagram sekwencji weryfikacji stempla czasowego