Cryptographic mechanisms in the e-prescription system

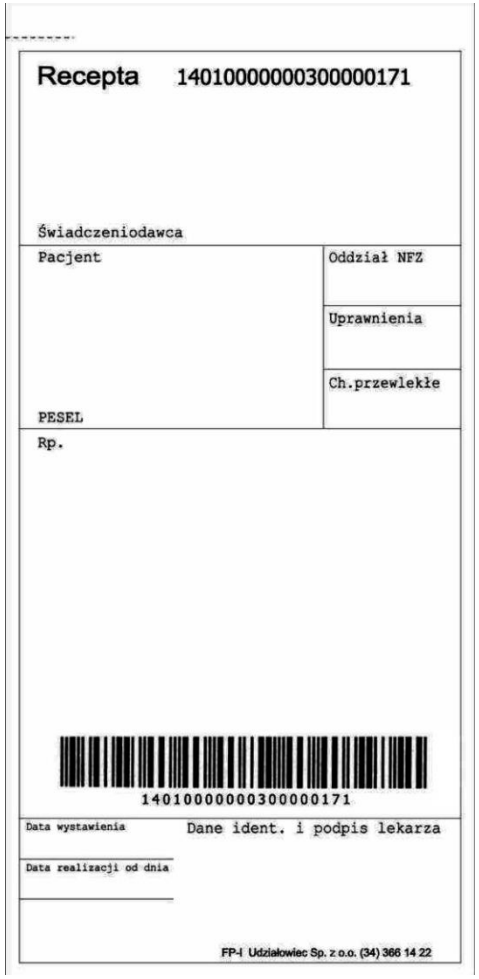
Author: Bartłomiej Słota

Supervisor: prof. dr hab. inż. Zbigniew Kotulski

Agenda

- Typical paper prescription
- The idea of the e-prescription system
- Engineer degree thesis aims
- Architecture
- Cryptographic mechanisms
- E-prescription object structure
- E-prescription life cycle
- Summary

Classical paper prescription


Recepta 14010000000300000171

Świadczeniodawca

Pacjent

Oddział NFZ

Uprawnienia

Ch.przewlekłe

PESEL

Rp.

14010000000300000171

Data wystawienia

Dane ident. i podpis lekarza

Data realizacji od dnia

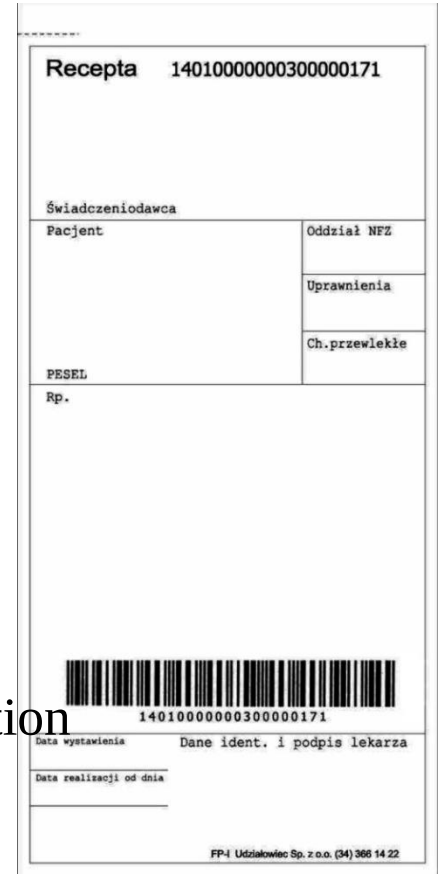
FP-I Udziałowiec Sp. z o.o. (34) 366 14 22

- Bar code and corresponding number
- Provider's information
- Patient's information (personal data, additional rights)
- Medicines (names, doses, etc.)
- Doctor's stamp and signature
- Date

The idea of the e-prescription system

Implementation should have similar features to the classical prescription:

- Legibility
- Durability
- Unambiguity
- Precision



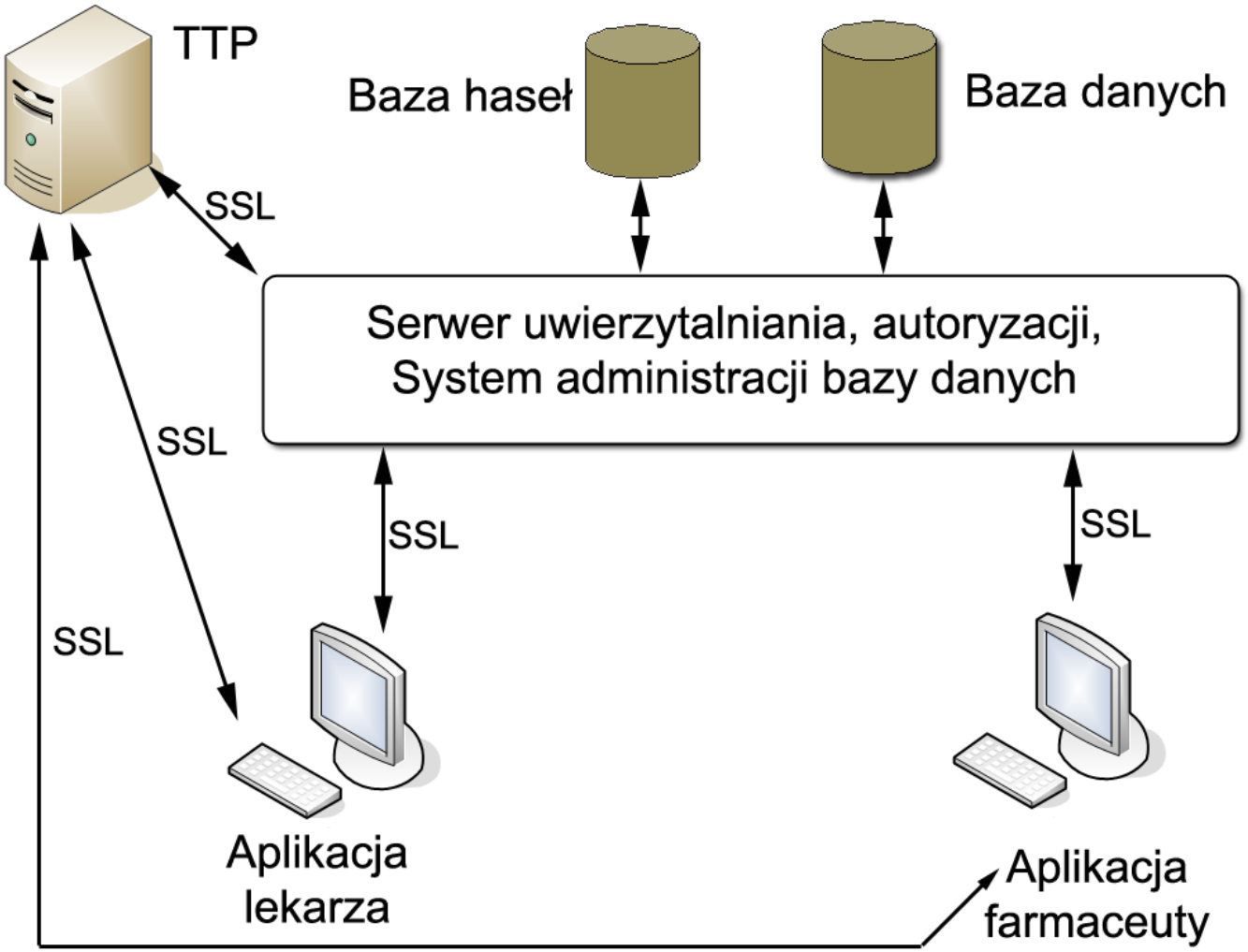
E-prescription system must ensure:

- Signature
- Authorization
- Decree-based data
- Generation of a document allowing to issue a prescription

Engineer degree thesis aims

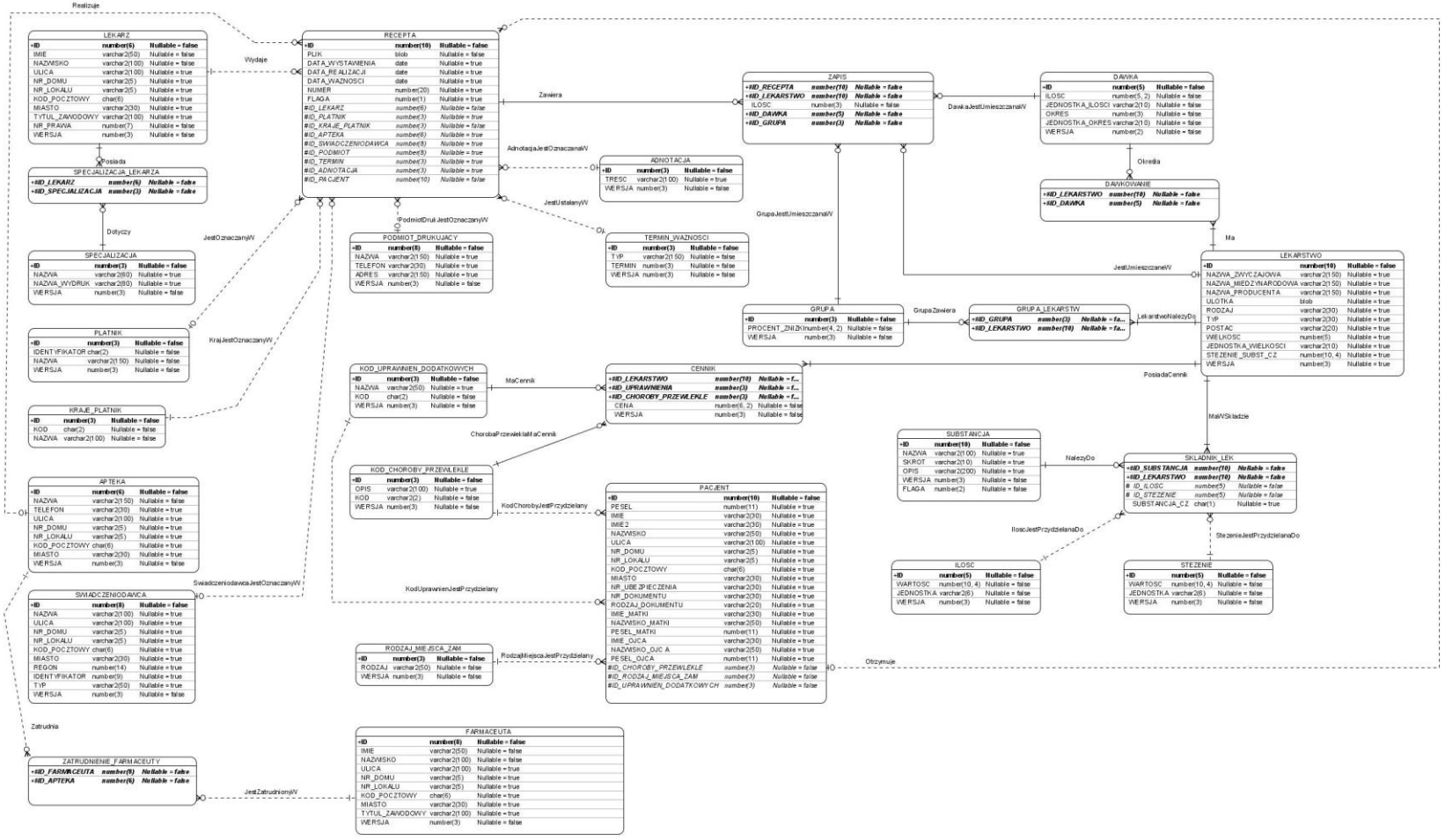
1. Implementation of an unambiguous, precise, and secure e-prescription object
2. Database capable of storing data about doctors, patients, pharmacist, drug stores, prescriptions.
3. Implementation of a system, which supports e-prescription generation, filling, and issuing.
4. Ensurance of the basic cryptographic services: authenticity, confidence, integrity, undeniability and access control

Architecture



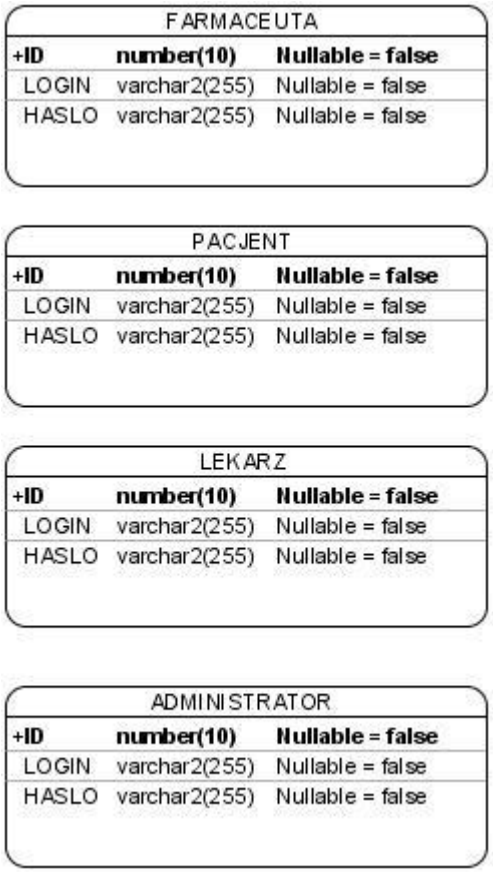
Architecture

Database



Architecture
Security database

- ID’s and password digests
- Basis of the users’ authenticity verification
- Security database separation from the database



Architecture
Middle layer(1/2)

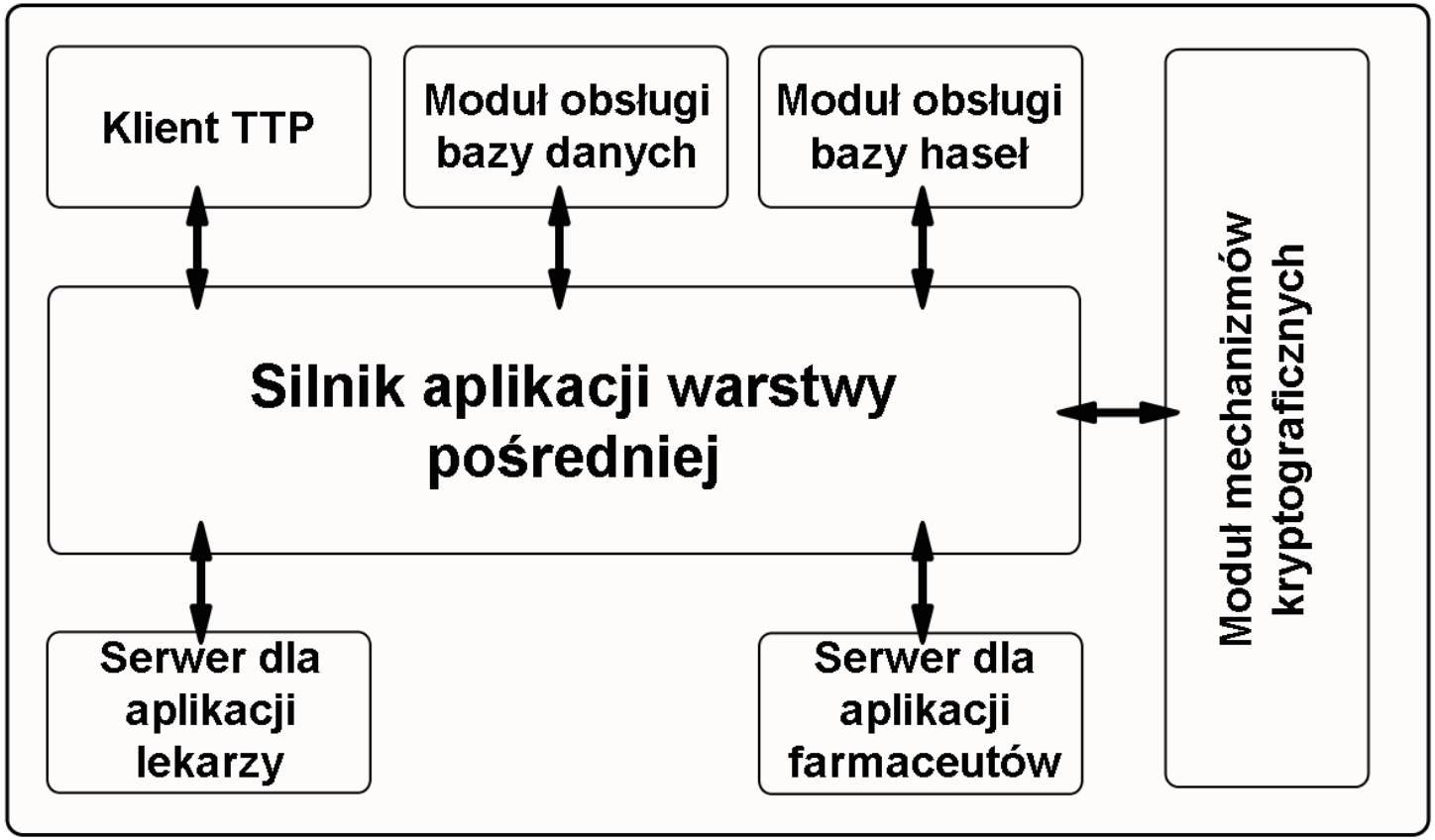
Database administration system

- Enables users to access proper read only data
- Generates e-prescriptions

Authentication and authorization server

- Authenticates doctors, pharmacists (and patients)
- Grants authorization to logged in users
- Analizes and updates logs

Architecture
Middle layer(2/2)

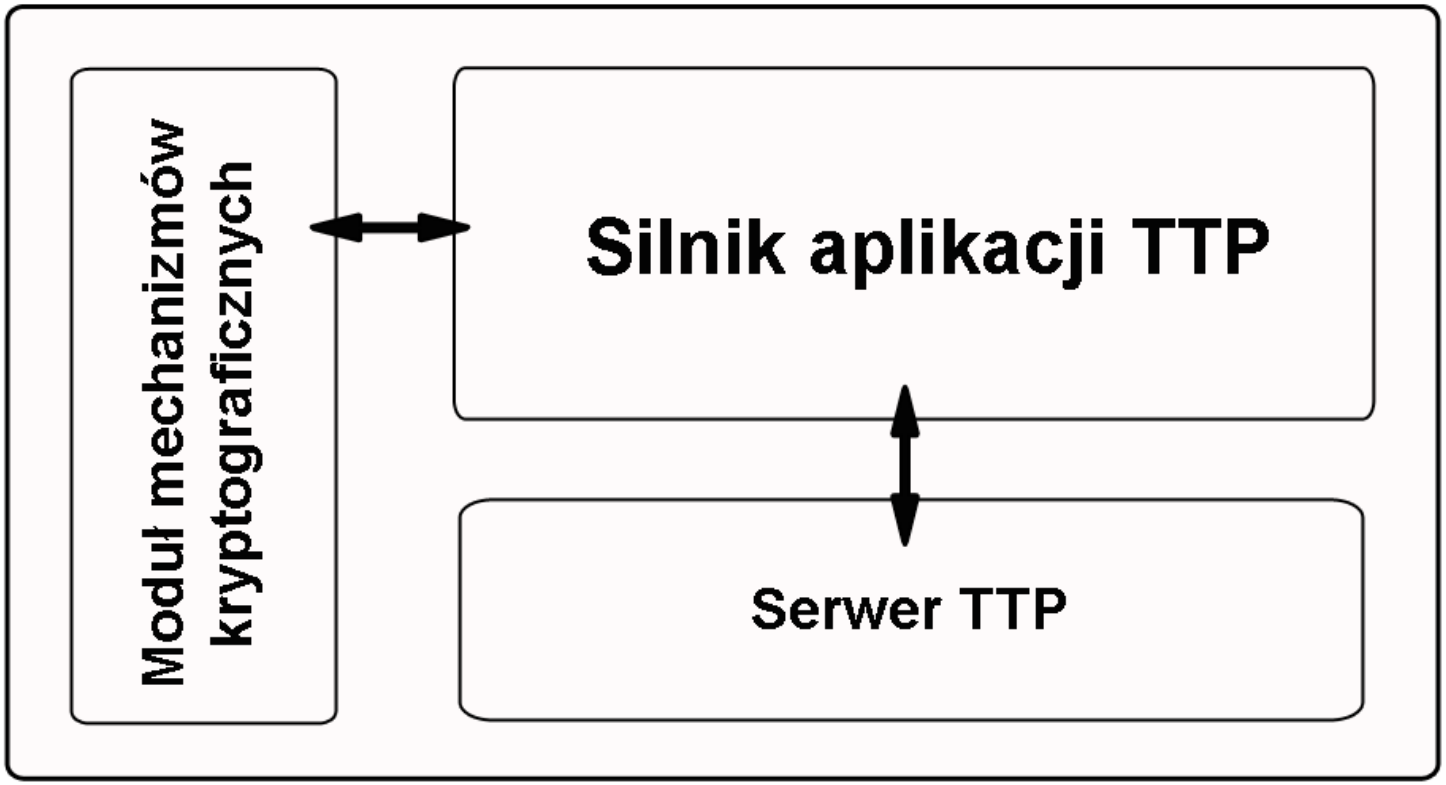


Architecture
Trusted Third Party - TTP (1/2)

- Generates digital certificates
- Manages Certificate Revocation List (CRL)
- Generates RSA key pair for the the users
- Uses OCSP (Online Certificate Status Protocol) to allow users to check whether the certificate they get is not revoked
- Generates password for the first login procedure (non-electronic)
- Users' private keys are stored in enciphered files on some external USB devices

Architecture

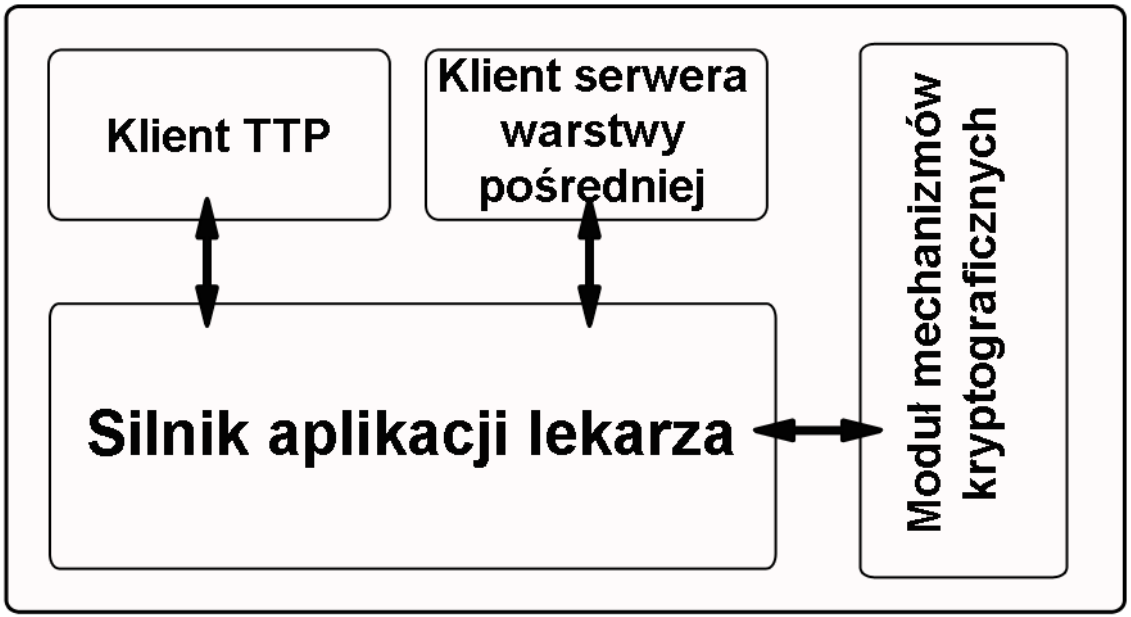
Trusted Third Party- TTP (2/2)



Architecture
Applications (1/2)

Doctor's application

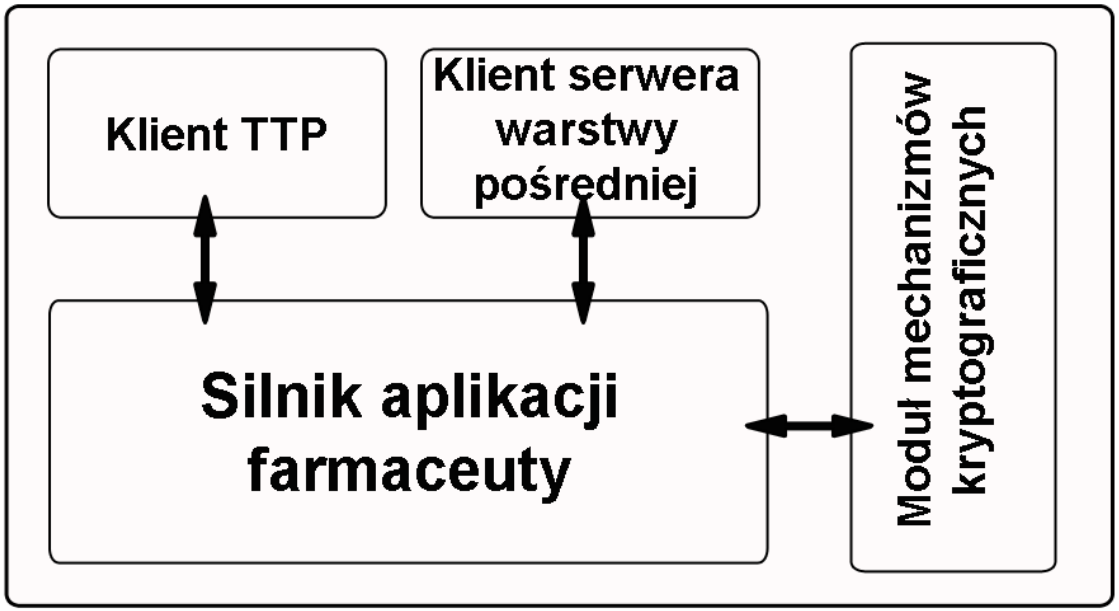
- Provides access to the information about medicines, doses, etc., and the basic information about the patient
- Supports filling e-prescriptions



Architecture
Applications (1/2)

Pharmacist's application

- Provides access to the information about medicines' doses, etc.
- Supports e-prescription issuance and dispensed medicines marking



Cryptographic mechanisms

Digital certificate

Digital signature

Secure SSL (TLS) channel

Authentication

Cryptographic mechanisms
Digital certificate(1/2)

- Public key digitally signed by Trusted Third Party
- Contains basic information about the certified user
- Unables key replacement
- Transmitted inside the body of e-prescription

Cryptographic mechanisms
Digital certificate (2/2)

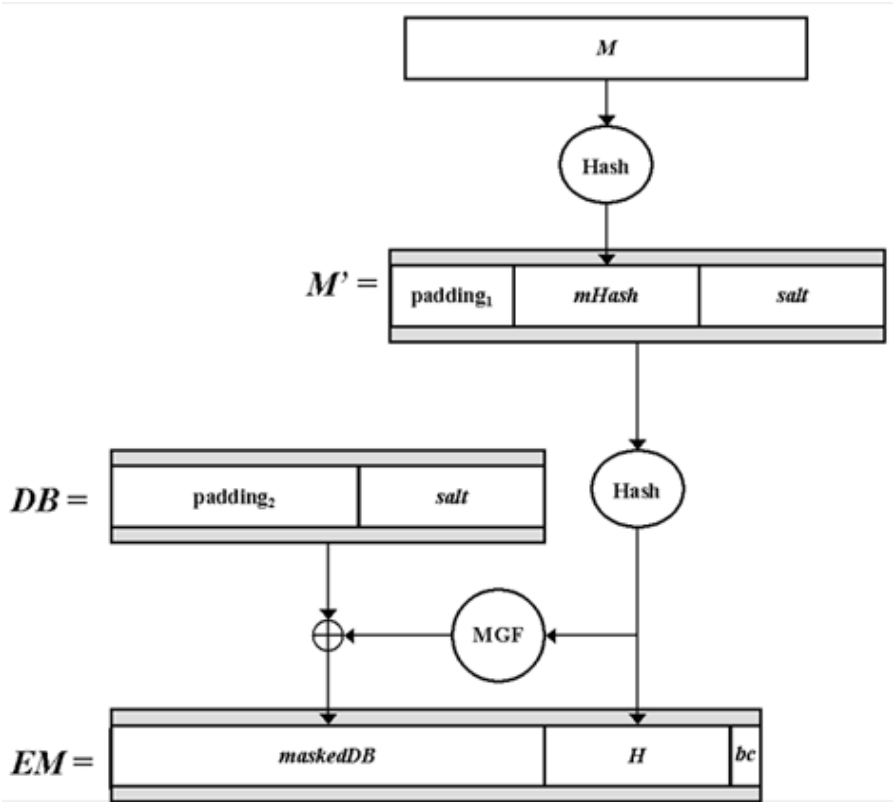
- Requeired from every user of the system
- TTP certificate
  - X.509 certificate, version 1.
  - trusted for every user of the system
  - enables verification of all certificates that can be used in the system
- Server (Middle Layer) certificate
  - X.509 certificate, version 1.
  - trusted for doctors and pharmacists, but not for TTP
- Doctors' and pharmacists' certificates
  - X.509 certificates, version 3.

Cryptographic mechanisms
Digital signature(1/2)

- RSA-PSS (Probabilistic Signature Scheme)
- Used in every transaction connected with an e-prescription object
- Can be verified using a digital certificate corresponding to the private key used by signature

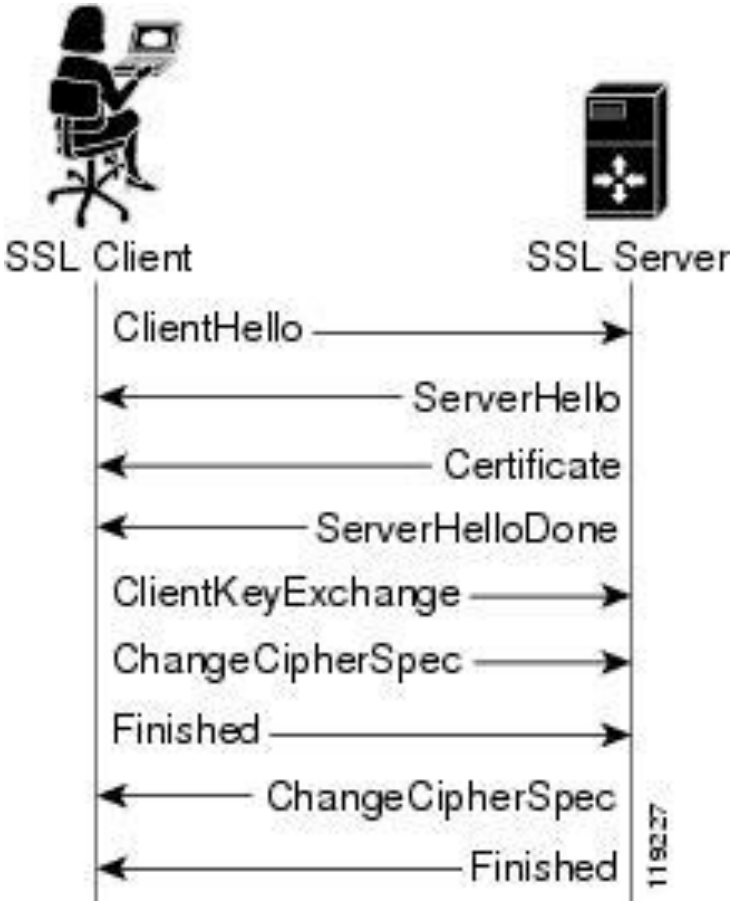
Cryptographic mechanisms
Digital signature (2/2)

- Its security can be related directly to the RSA problem (factoring the modulus)
- PSS is „provably secure”, which corresponds to the current trend
- The message randomization, which plays an important role in increasing security level



Cryptographic mechanisms
Secure SSL channel

- A set of cryptographic protocols that provide communication security over the Internet
- Handshake protocol
- Not using client-authenticated handshake!

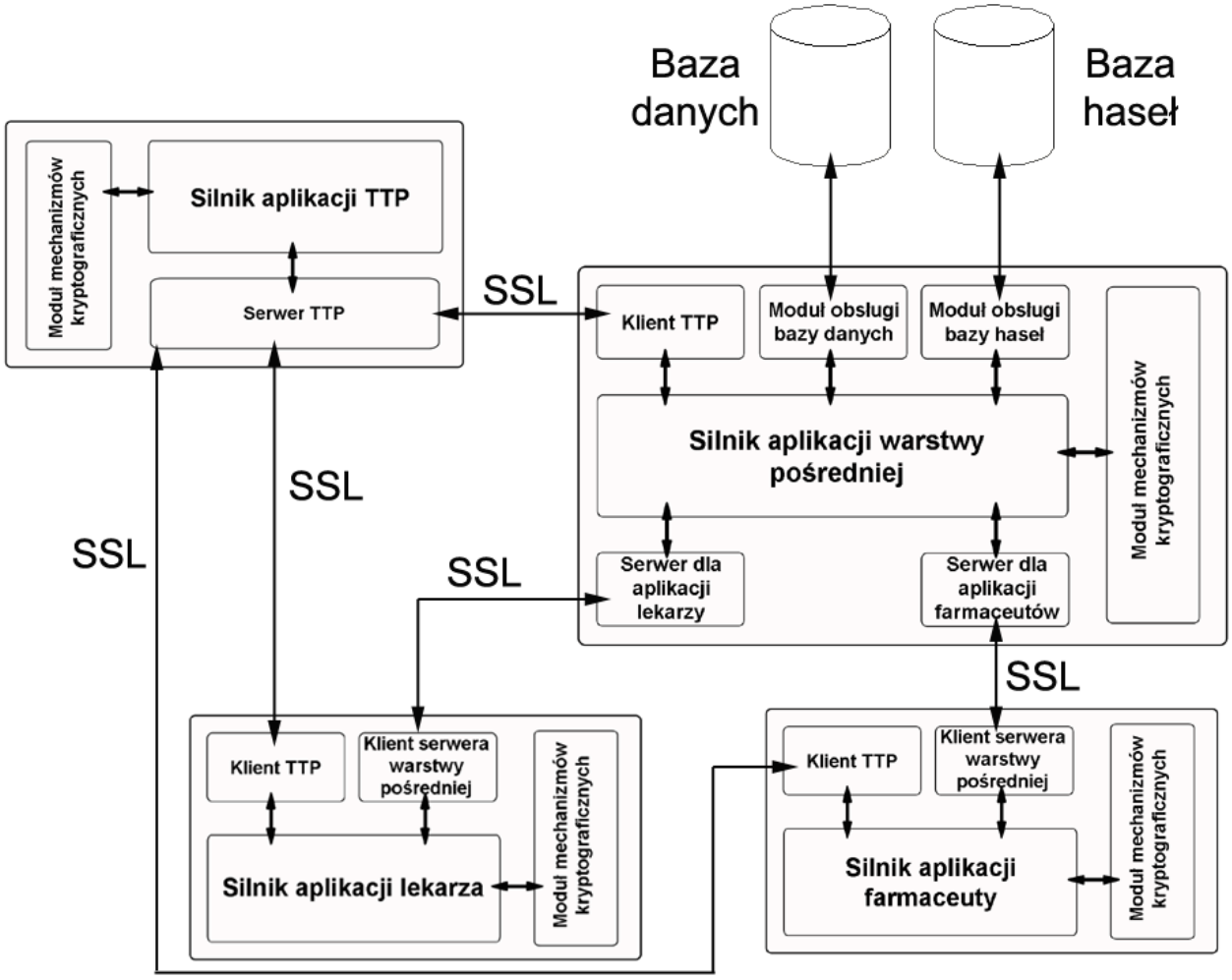


Źródło: CISCO

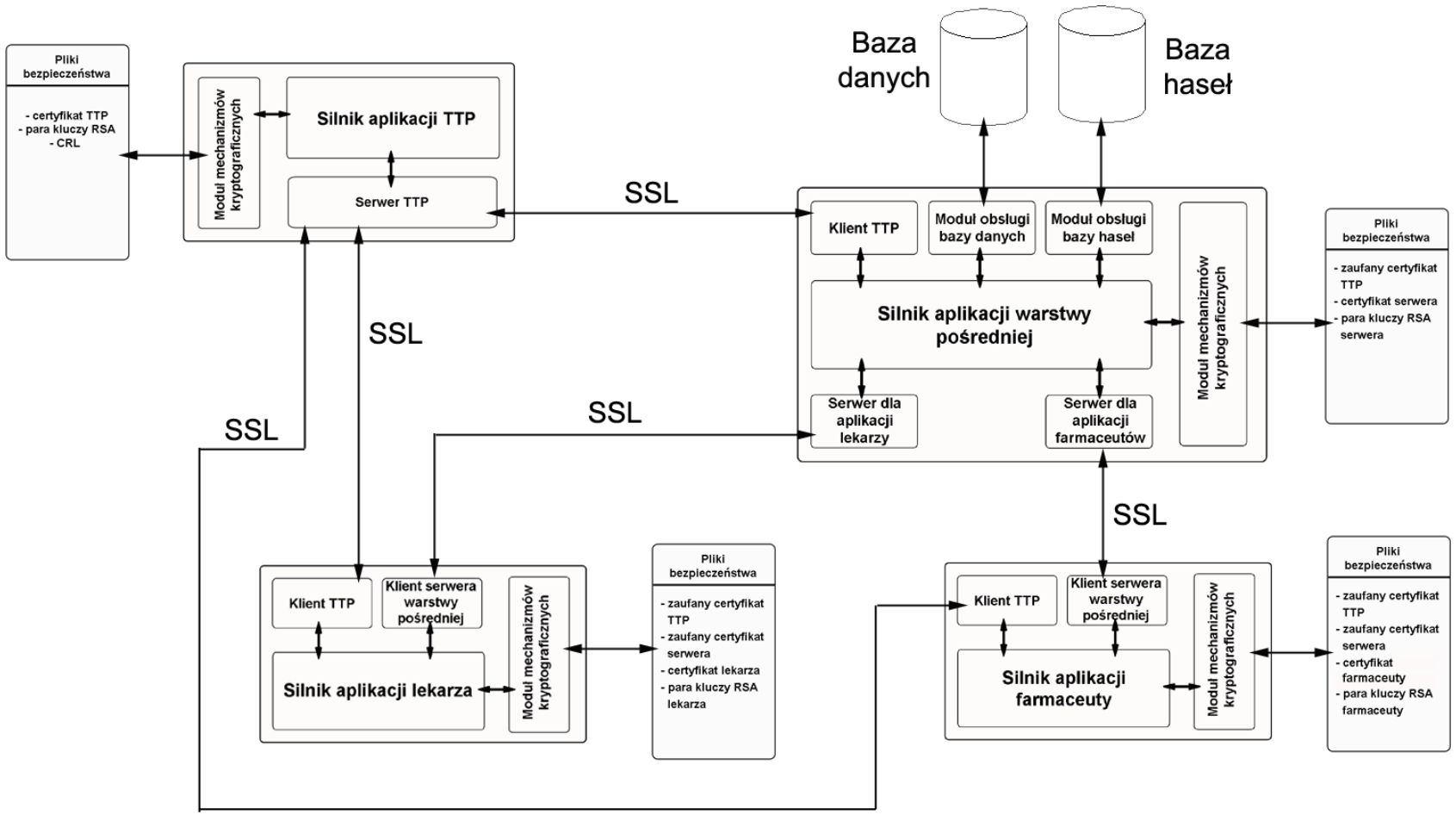
Cryptographic mechanisms
Authentication

- Authenticity verification of the logging user (doctor, pharmacist, server administrator, TTP administrator, and patient…)
- Login and password are sent via secure channel to the middle layer application
- Received password hash is compared with the one stored in the security database
- The whole process is constantly supervised by the middle layer (as everything in the system network)

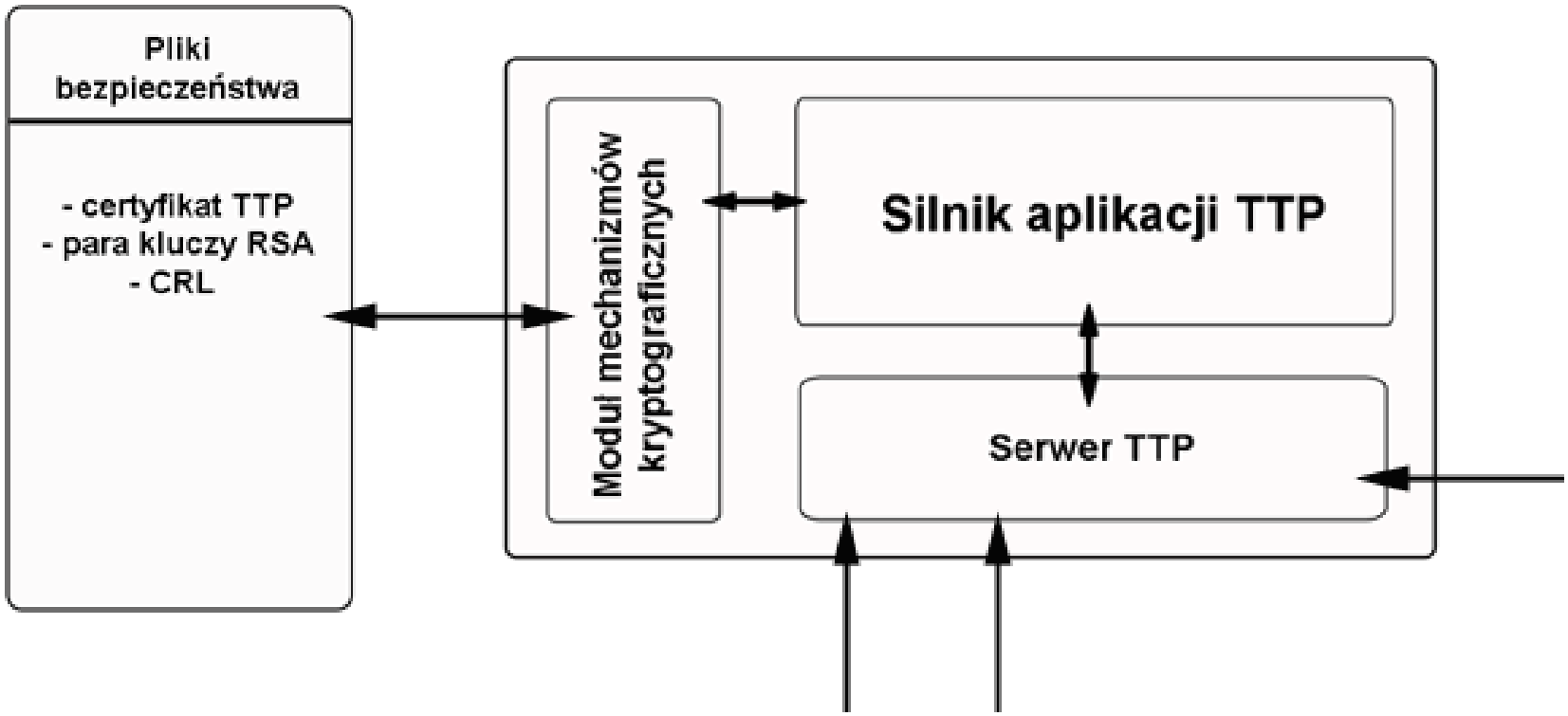
Functional architecture (1/6)



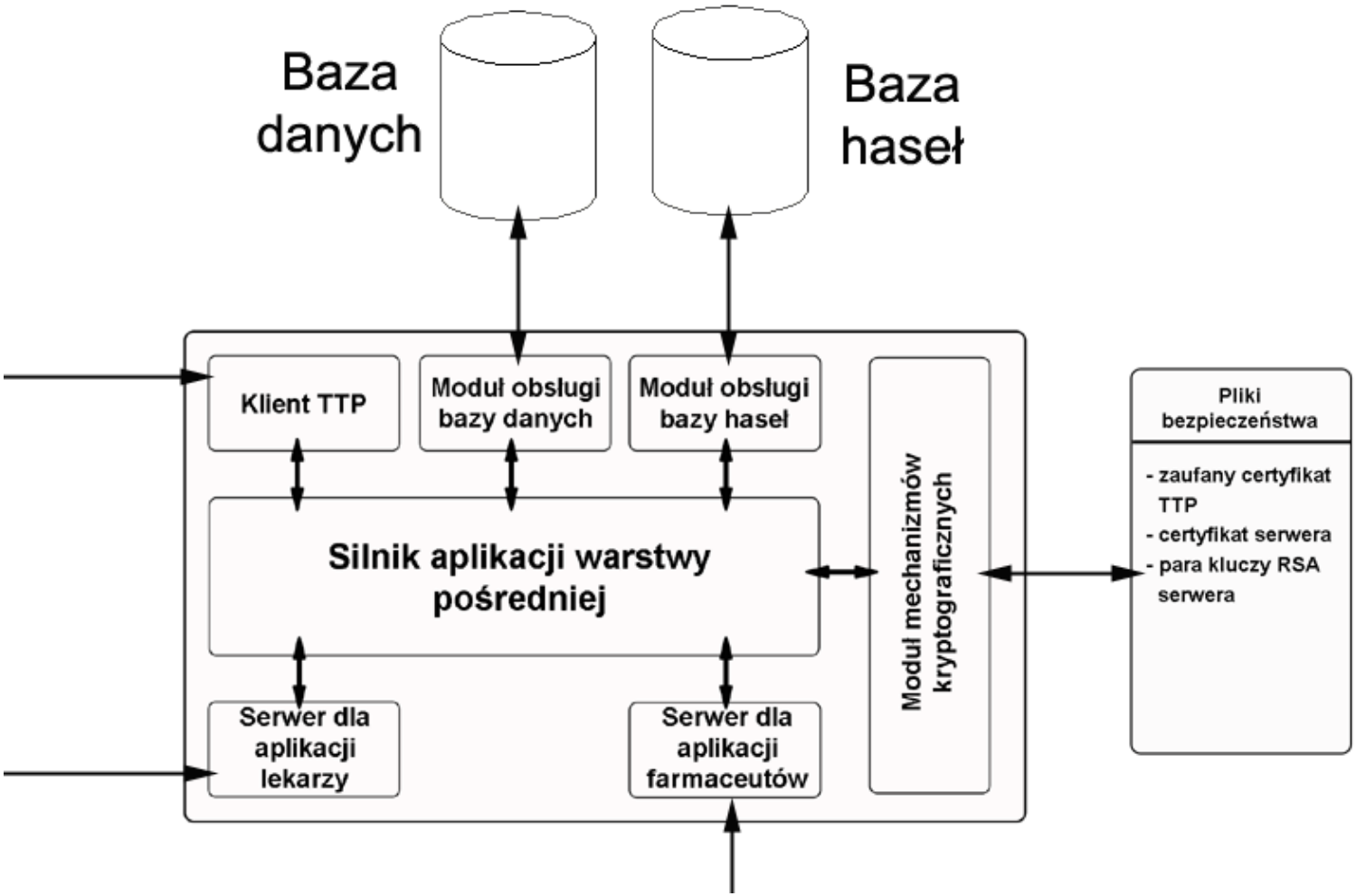
Functional architecture (2/6)



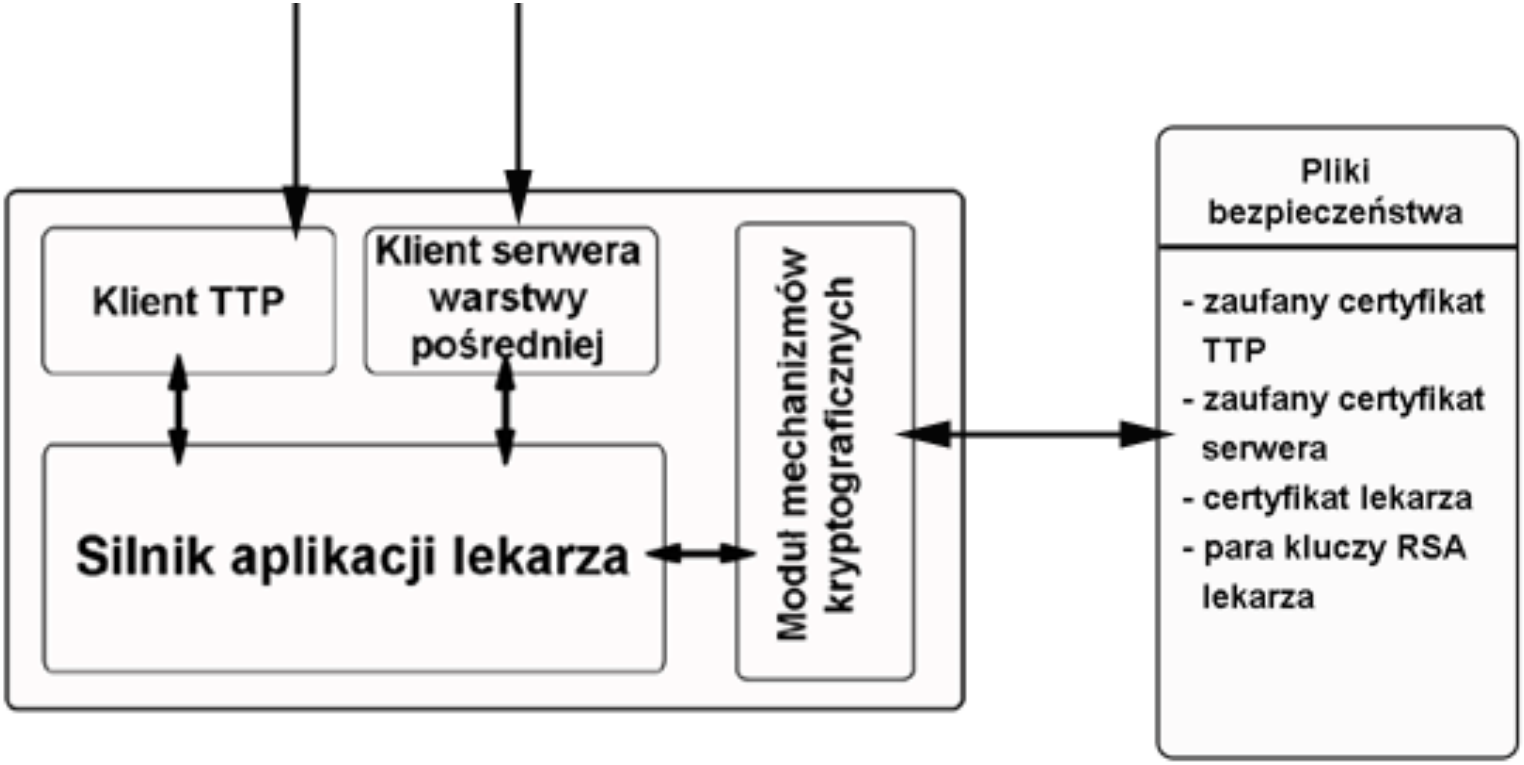
Functional architecture (3/6)



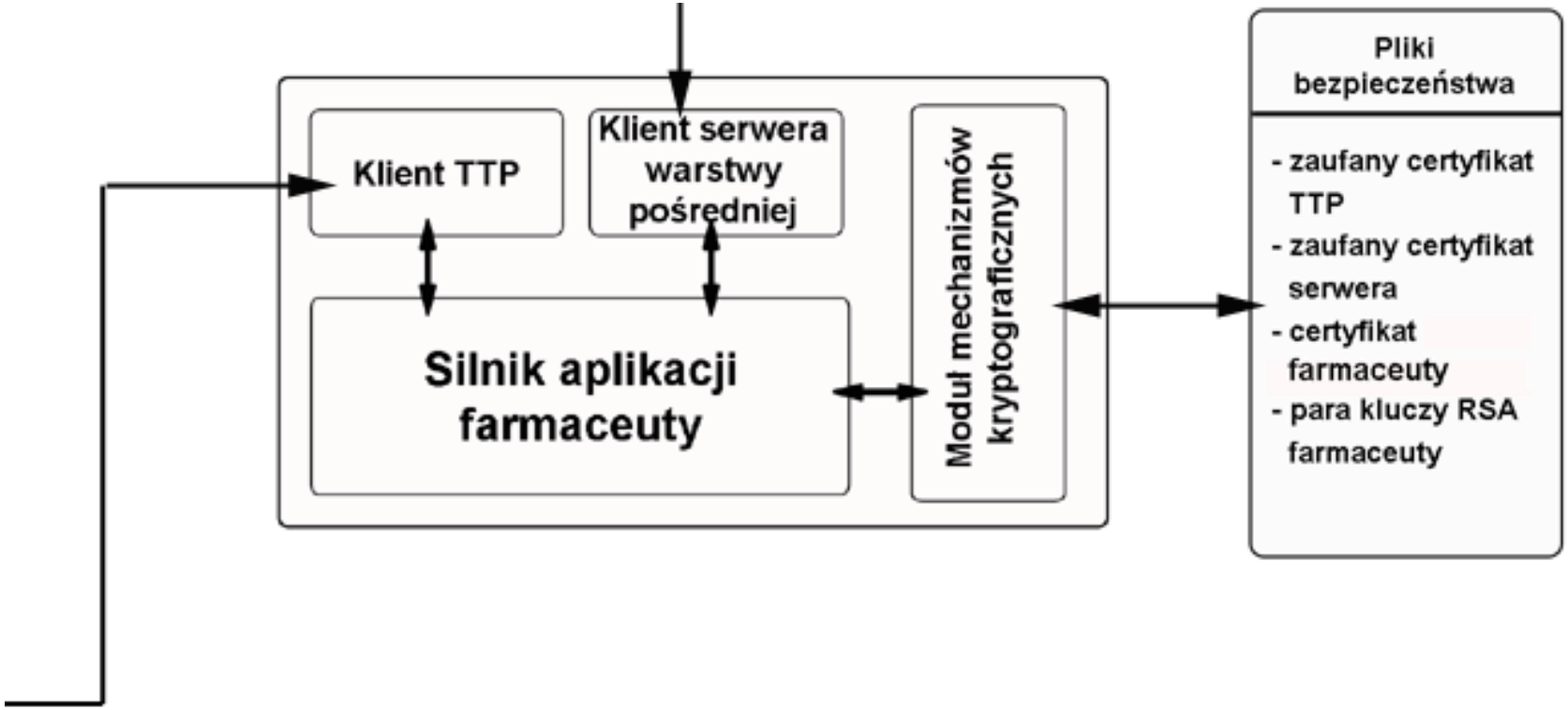
Functional architecture (4/6)



Functional architecture (5/6)



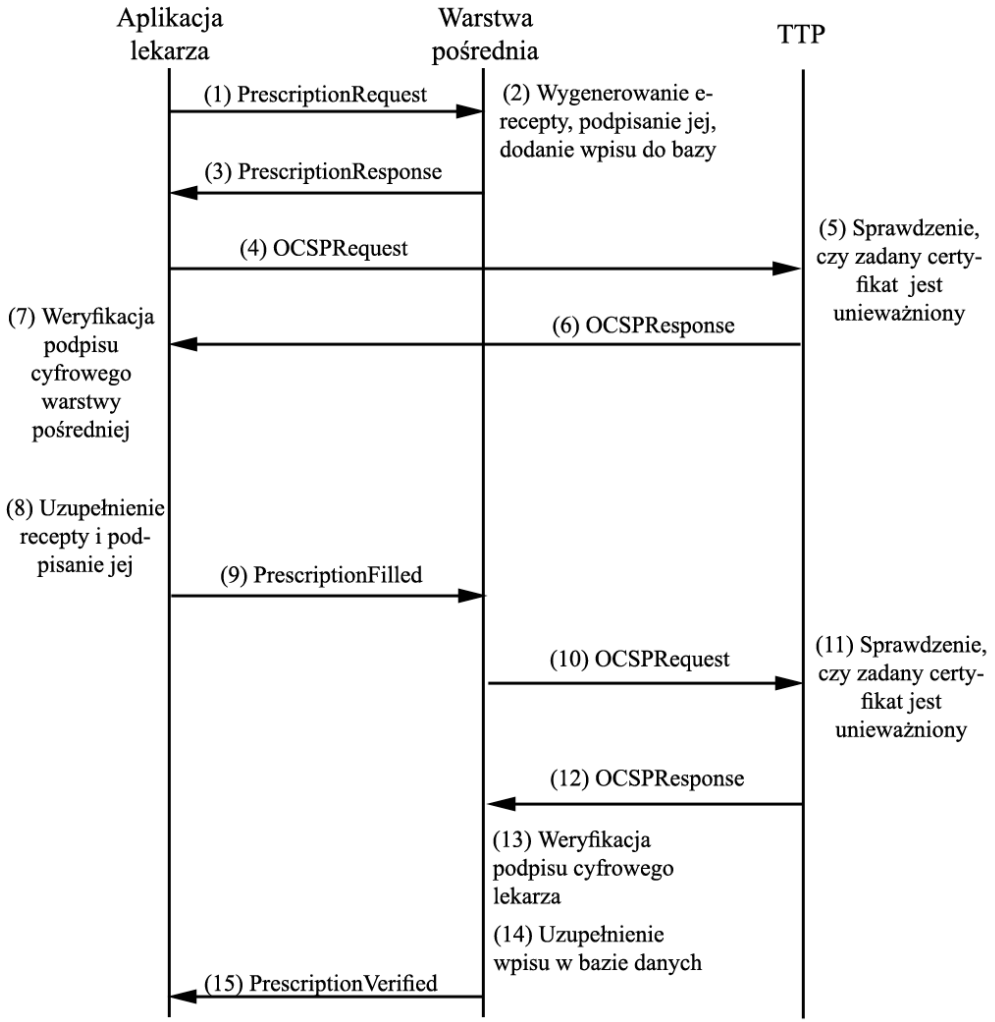
Functional architecture (6/6)



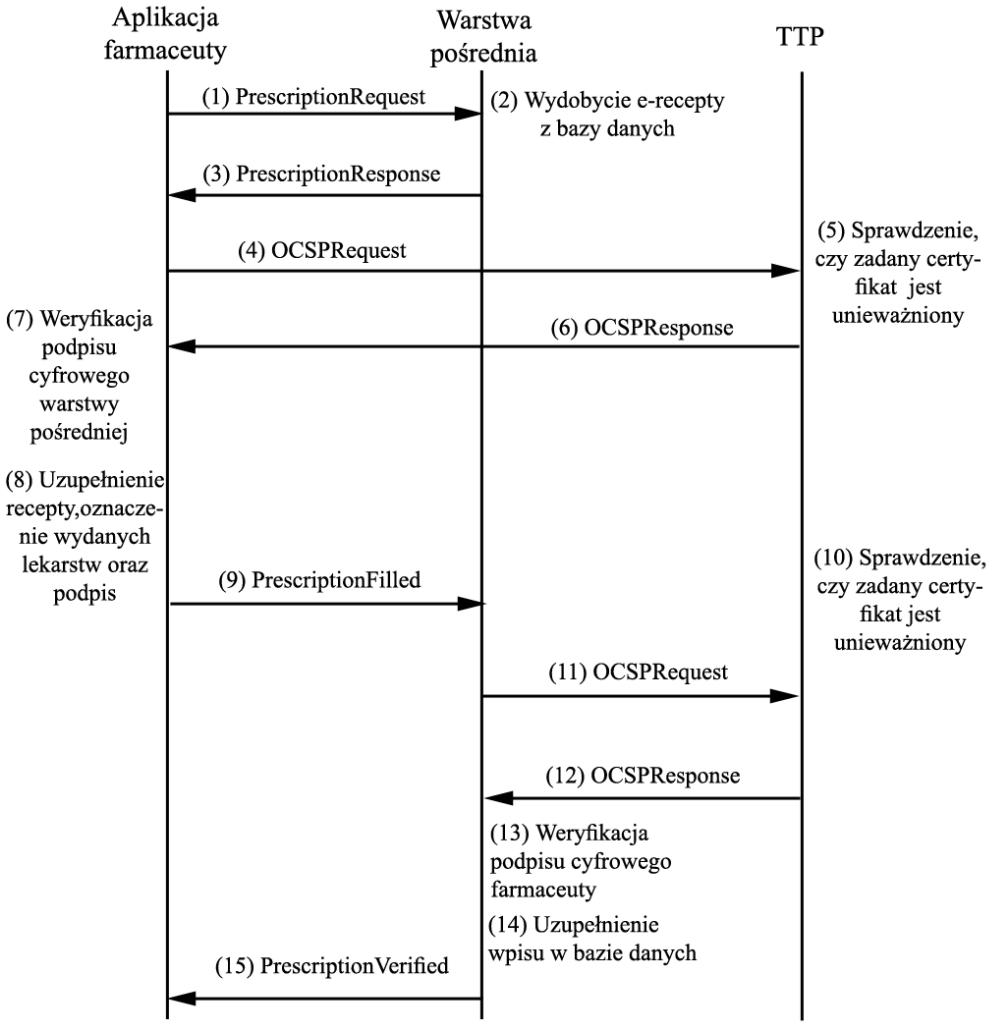
E-prescription object structure

- XML file, that contains data, which are similar to those placed on the classical paper prescription
- Firstly, it is generated from the template
- Systematically filled and digitally signed by subsequent users – high integrity level!
- Transfers PEM certificates.

E-prescription life cycle (1/2)



E-prescription life cycle (2/2)



Summary

- System ensures: authenticity, confidence, integrity, undeniability and access control – basic cryptografic services
- Innovative project
- Elastic architecture

Thank you!