TriNova

INTEL UNNATI TRAINING

SUMMER INTERNSHIP - 2024

Team Members :

Maitri Rajesh Dulla
Ayushi Meshram
Sakshi Sunil Pawar

TABLE OF CONTENT

- Problem Statement
- Unique Idea Brief
- Features Offered
- Process Flow
- Architecture Diagram
- Technologies Used
- Team members and Contribution
- Conclusion

PROBLEM STATEMENT

Cryptography Simulation with mbedTLS/OpenSSL Library Usage and User Interaction.

UNIQUE IDEA BRIEF (SOLUTION)

To develop an interactive cryptography simulation platform using mbedTLS or OpenSSL libraries. The platform will enable users to establish secure connections between servers and clients, ensuring that third parties cannot access the communication. The conversation can only be decrypted or analyzed using the corresponding key. Additionally, the platform will provide functionalities for secure key exchange, encryption and decryption processes, and simulation of various cryptographic scenarios to enhance users' understanding of secure communication protocols.

FEATURES OFFERED

- **Interactive Real-Time Simulations:** Live demonstrations illustrating cryptographic processes such as encryption/decryption, digital signing, and verification for enhanced learning.
- **Support for Multiple Algorithms:** Includes AES, RSA, DH, and other cryptographic algorithms to cater to diverse security needs and preferences.
- **Advanced Security Analysis Tools:** Tools for visualizing and evaluating the security implications of different cryptographic choices, aiding in informed decision-making.

- **Seamless Cross-Platform Compatibility**: Compatible with Windows, macOS, and Linux, ensuring accessibility across various operating systems.

- **Integration with Leading Libraries**: Integration with mbedTLS and OpenSSL for reliable and proven implementations of cryptographic functions, ensuring robust security standards.

PROCESS FLOW

1. Install OpenSSL and Wireshark: Set up both the OpenSSL library and Wireshark on your system.

2. Generate Certificates: Create certificates and ensure they are properly linked.

3. Extract and Open Project: Unzip the provided file and open it in Visual Studio.

4. Initialize OpenSSL in Visual Studio: Configure the OpenSSL library files and set their paths in Visual Studio.

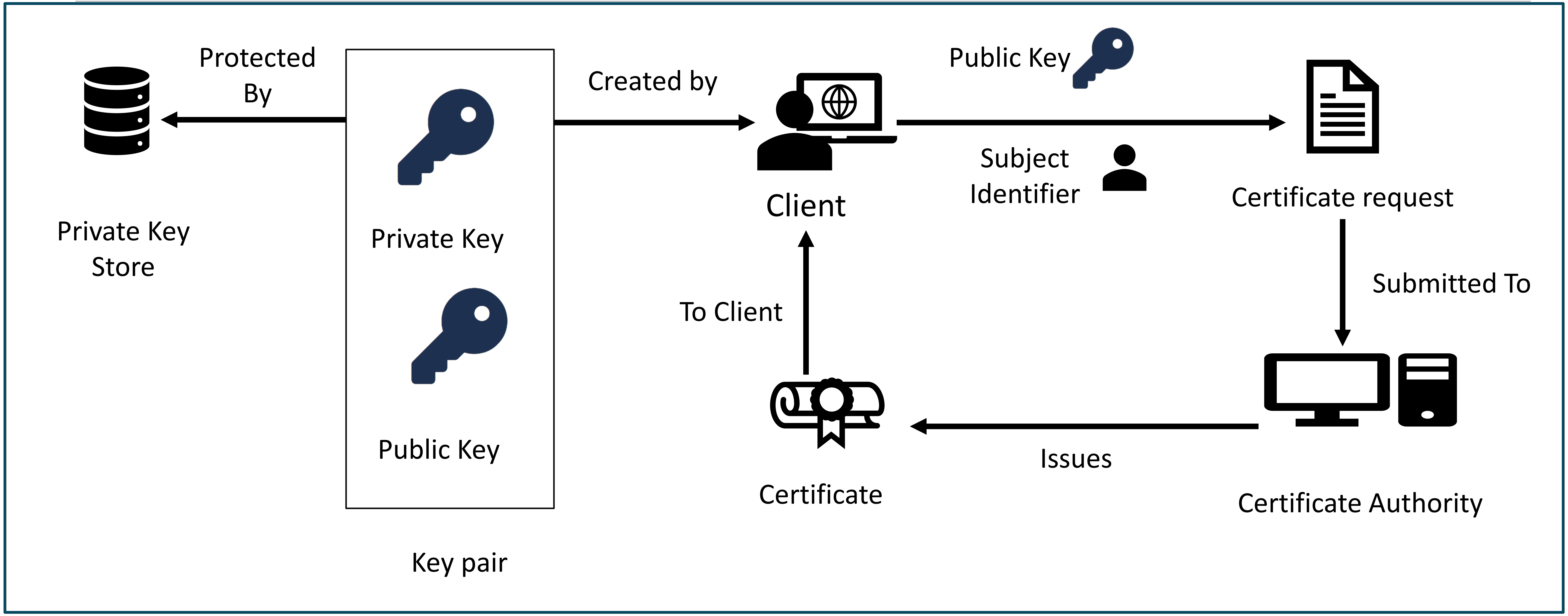
5. Develop and Test Code: Write the necessary C++ files and perform test passes to create a chat bot that operates in the command prompt

6. Monitor Chat Traffic: Use Wireshark to track the chat in its encrypted format.

7. Decrypt Chat: Decrypt the chat using the private key that was generated during tracking.

8. Objective: The primary goal of these exercises is to create secure traffic between a client and a server.

ARCHITECTURE DIAGRAM



TECHNOLOGIES USED

Cryptographic Libraries :

- OpenSSL

Programming Languages :

- C++

Softwares :

- Wireshark
- Visual Studio 2022

System Resources:

- Command Prompt

TEAM MEMBERS AND CONTRIBUTION

- **Maitri Dulla** - Certificate Generation, Coding, Documentation
- **Ayushi Meshram**- Installation & Coding, Presentation
- **Sakshi Pawar**- Coding & Presentation, Resources searcher

CONCLUSION

Using OpenSSL or mbedTLS libraries, the interactive cryptography simulation platform provides a reliable and practical way to create secure connections between a client and a server. This ensures that all interactions are encrypted, shielded from prying eyes, and can only be decrypted with the appropriate keys. The platform offers users invaluable practical experience and deep insights into the crucial role cryptography plays in protecting digital communications, leveraging our extensive knowledge in cryptographic implementations and secure communication protocols.

THANK YOU