MCA-722
Project Presentation
MAY 2022

Certificate Generator

Utkarsh Gupta (192120009)

Internal Supervisor

Dr. Sanjay Sharma
Professor
Maulana Azad National Institute of Technology
Bhopal

External Supervisor

Mr. Pankaj Choudhary
Senior Technical Lead
Truminds Software Systems
Gurugram

Company Profile

Truminds

Software Systems

San Diego| Greater Boston | Gurgaon | Hyderabad | Bangalore
www.truminds.com

B2B | Licensable Software | Networking | AR | AI

Video Conferencing Platform

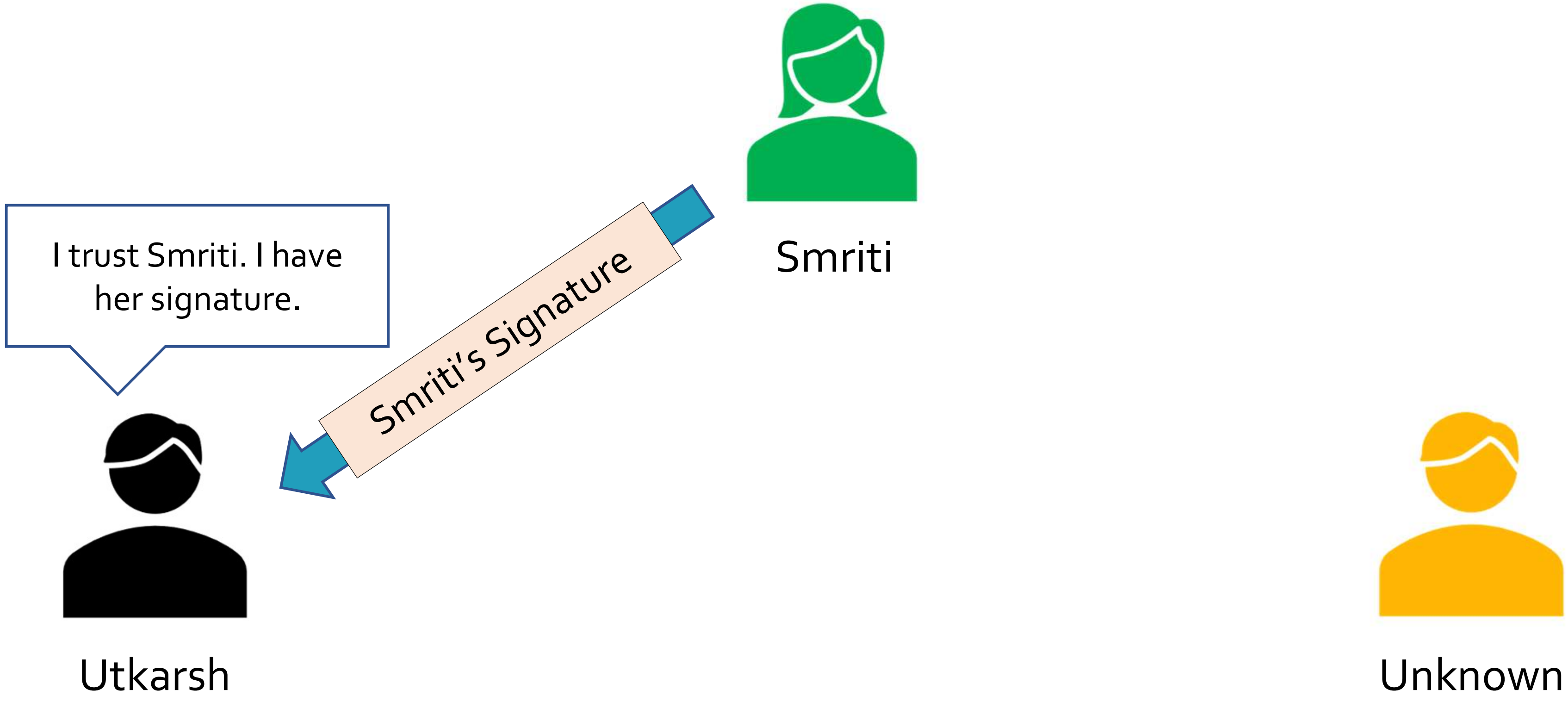
Online Exams Proctoring System

Large Scale Indoor Mapping

Network Traffic Routing Solution

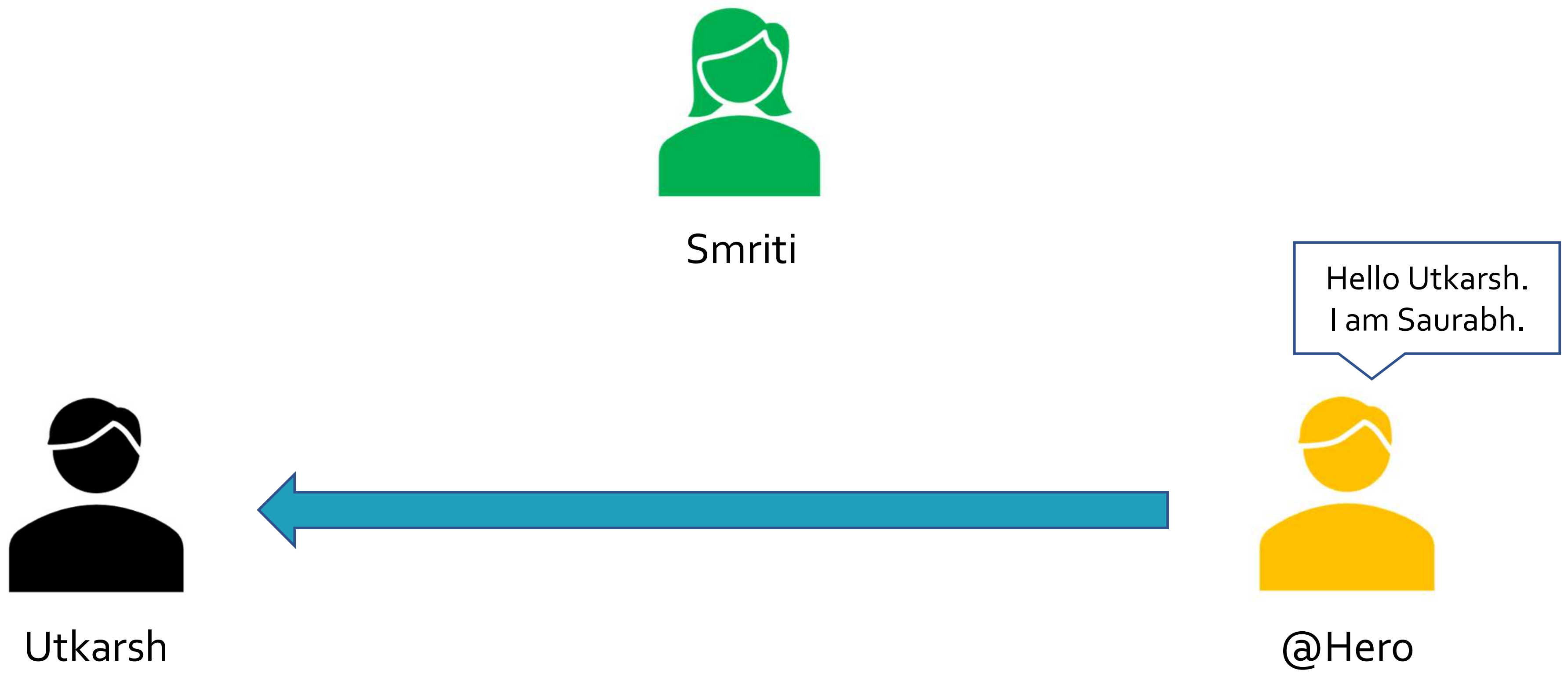
Digital Certificates

Trust based identity



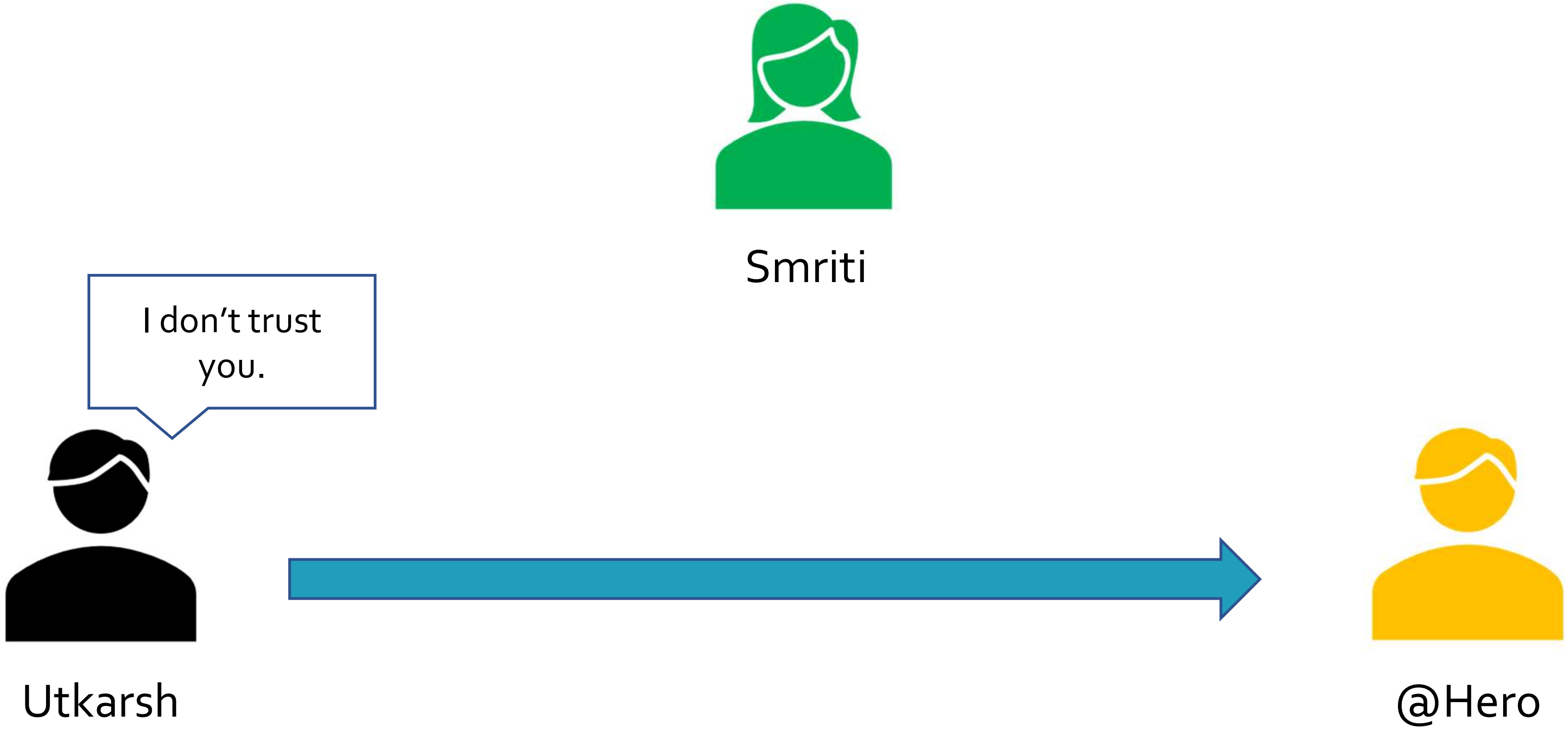
Digital Certificates

Trust based identity



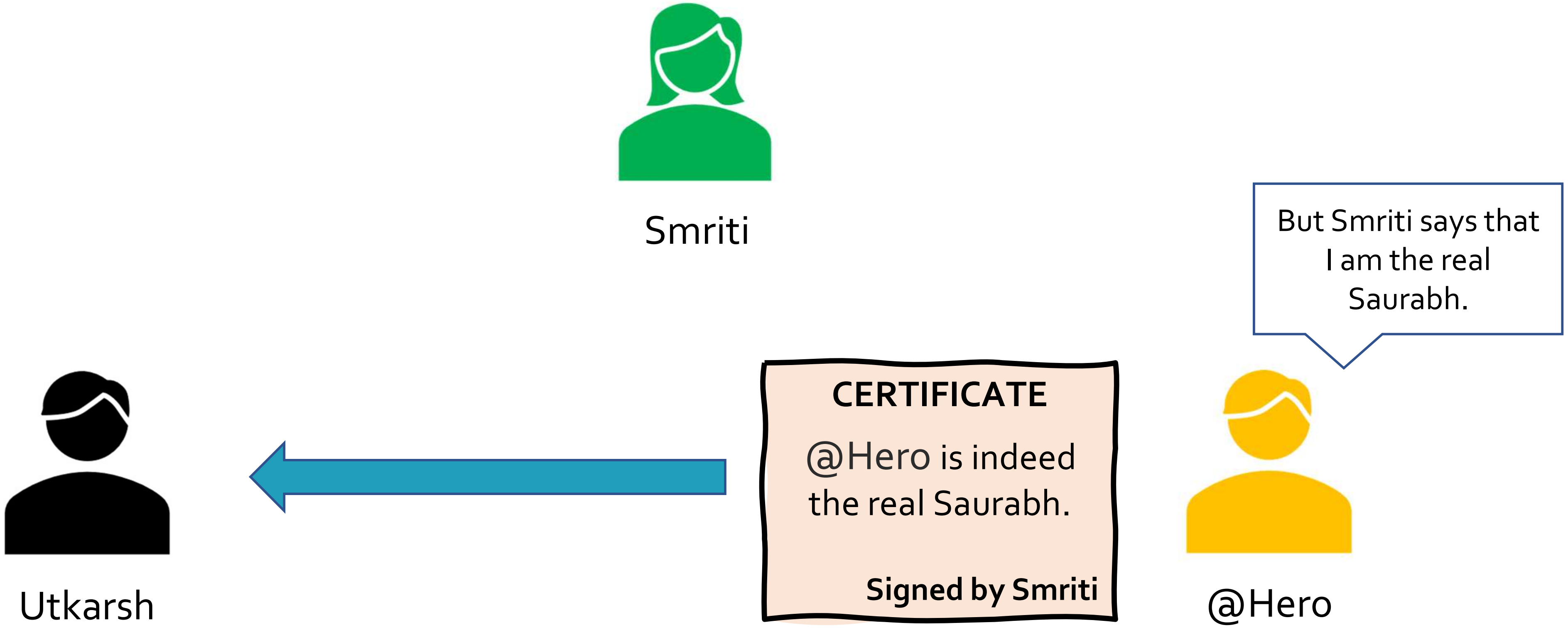
Digital Certificates

Trust based identity



Digital Certificates

Trust based identity



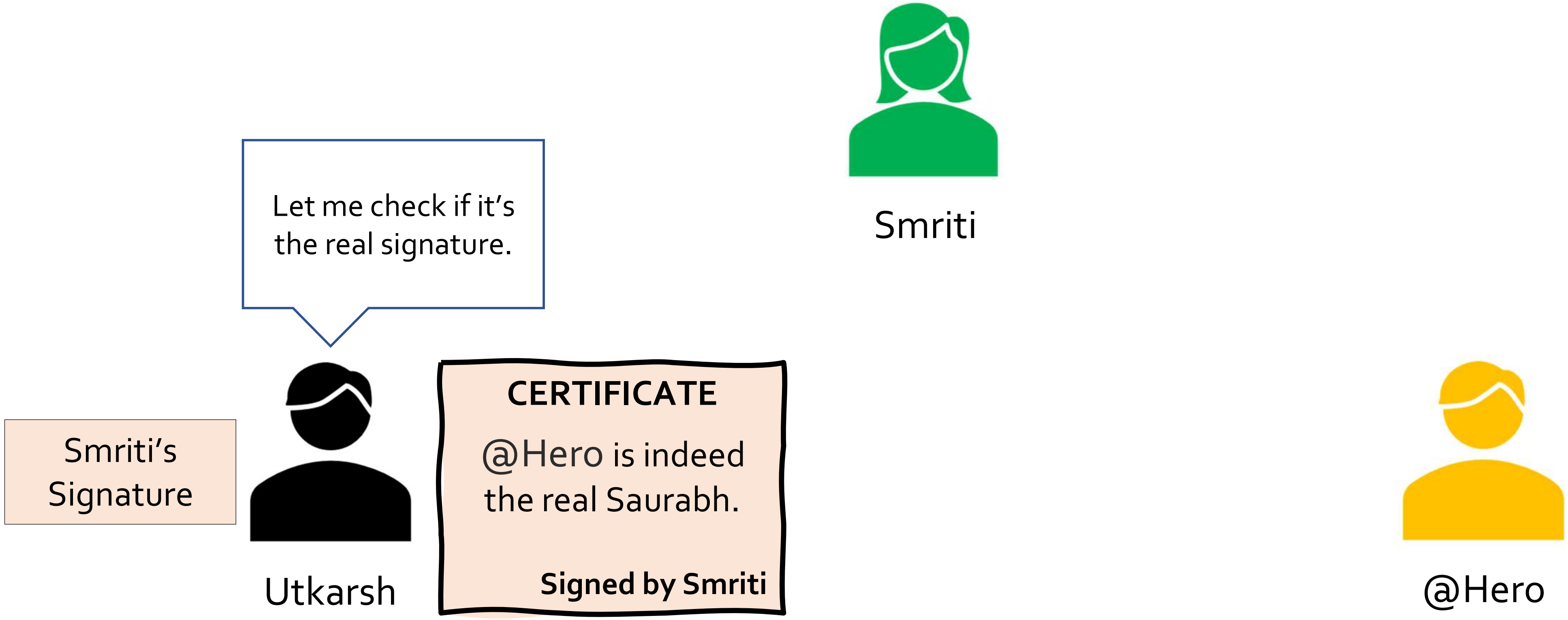
CERTIFICATE

@Hero is indeed the real Saurabh.

Signed by Smriti

Digital Certificates

Trust based identity



Let me check if it's the real signature.

Smriti

Smriti's Signature

Utkarsh

CERTIFICATE

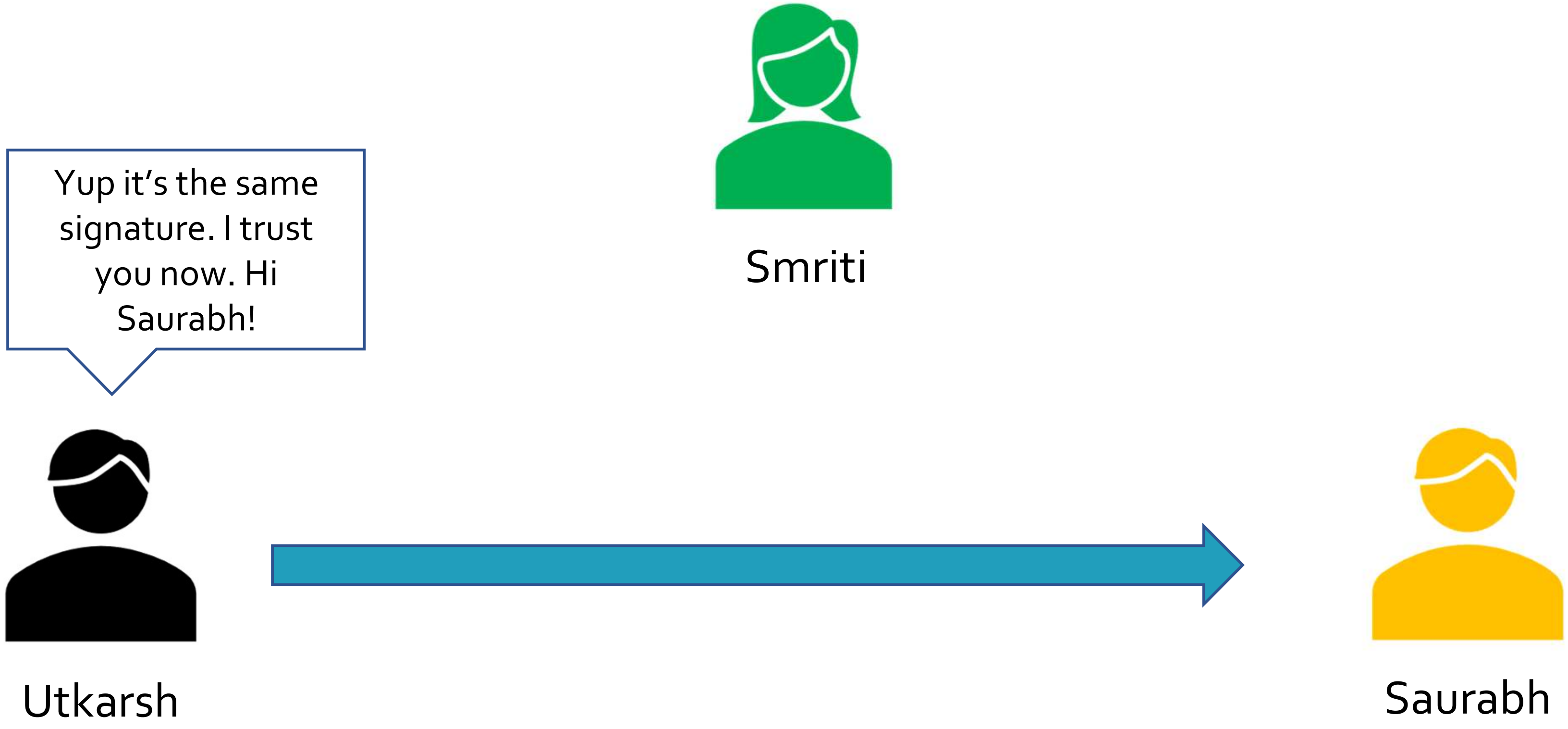
@Hero is indeed the real Saurabh.

Signed by Smriti

@Hero

Digital Certificates

Trust based identity



Digital Certificates

Secure

“Signature” is a metaphor.

It’s an encryption key (a pair of keys) that provide the "signature-ness".

There is no concept of “forging” a signature.

DIGITAL CERTIFICATE

Name: Saurabh
Locality: Sector 18 Gurugram
State: Haryana
Country: IN
Hostname: `realSaurabh.com`
Validity: 06/02/2022 to 17/02/2022

SIGNED BY SMRITI’S PRIVATE KEY

Certificate Generator

Digital Certificates Made Easy!

Certificate Generator

Graphical UI

Command Line

Python Libraries

Requirements

Senior Executive

- Knows absolute basics of what a Digital Certificate is.
- Wants an easy & quick way to create & sign certificates.
- Doesn't need many customization options.
- Has never used a Console.

.....

Project Manager

- Knows about digital certificates and encryption keys.
- Wants to quickly create or sign certificates in bulk quantities.
- Knows shell scripting.
- Needs some customizability.

.....

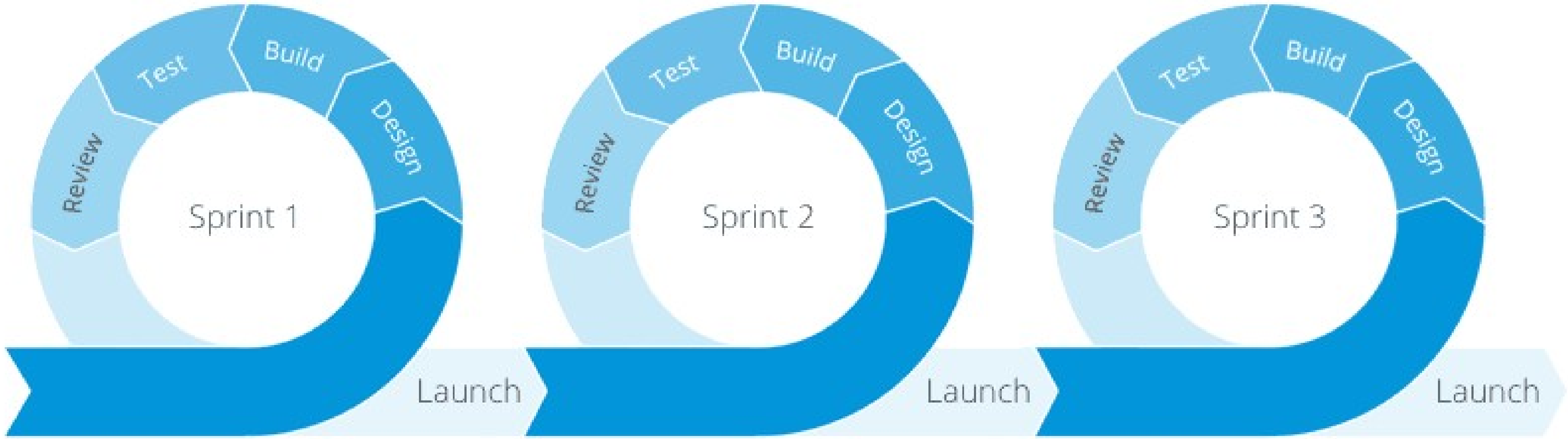
Backend Developer

- Knows exactly what goes into creating a certificate.
- Wants to embed digital certificate related functionality in his own project.
- Needs as much customization as possible.
- Knows programming.

.....

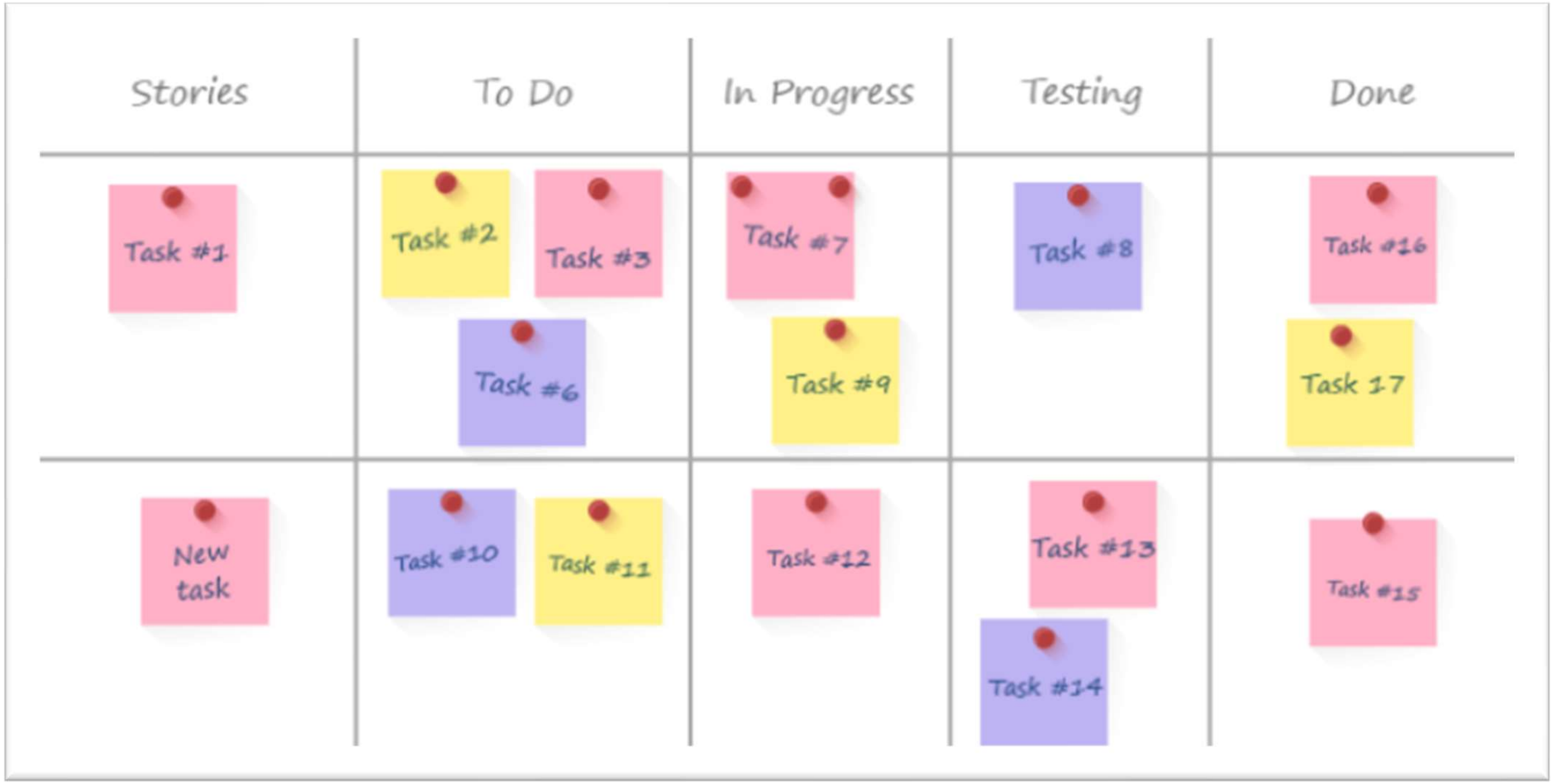
Action Plan

Agile Methodology



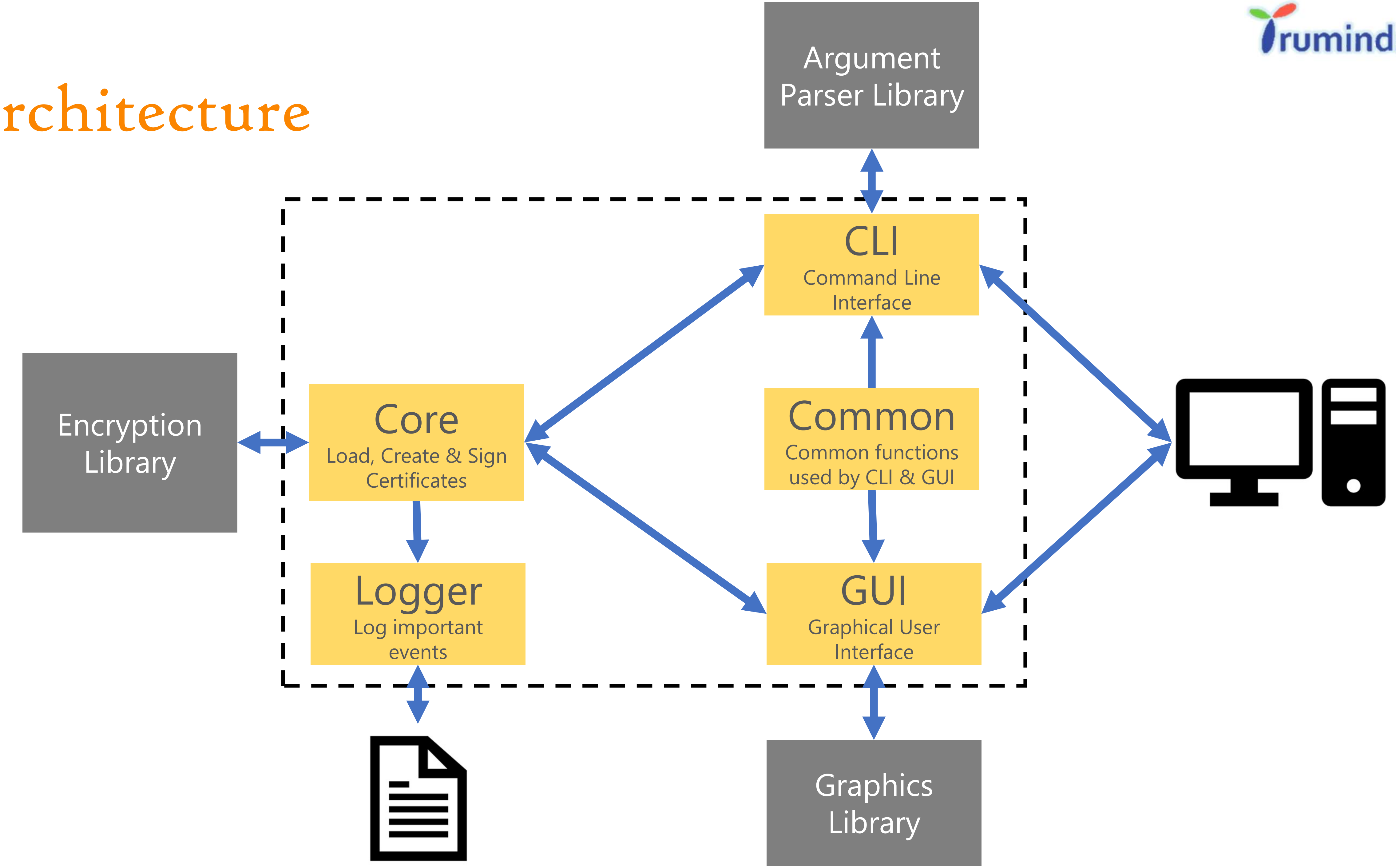
Action Plan

Kanban Tracking

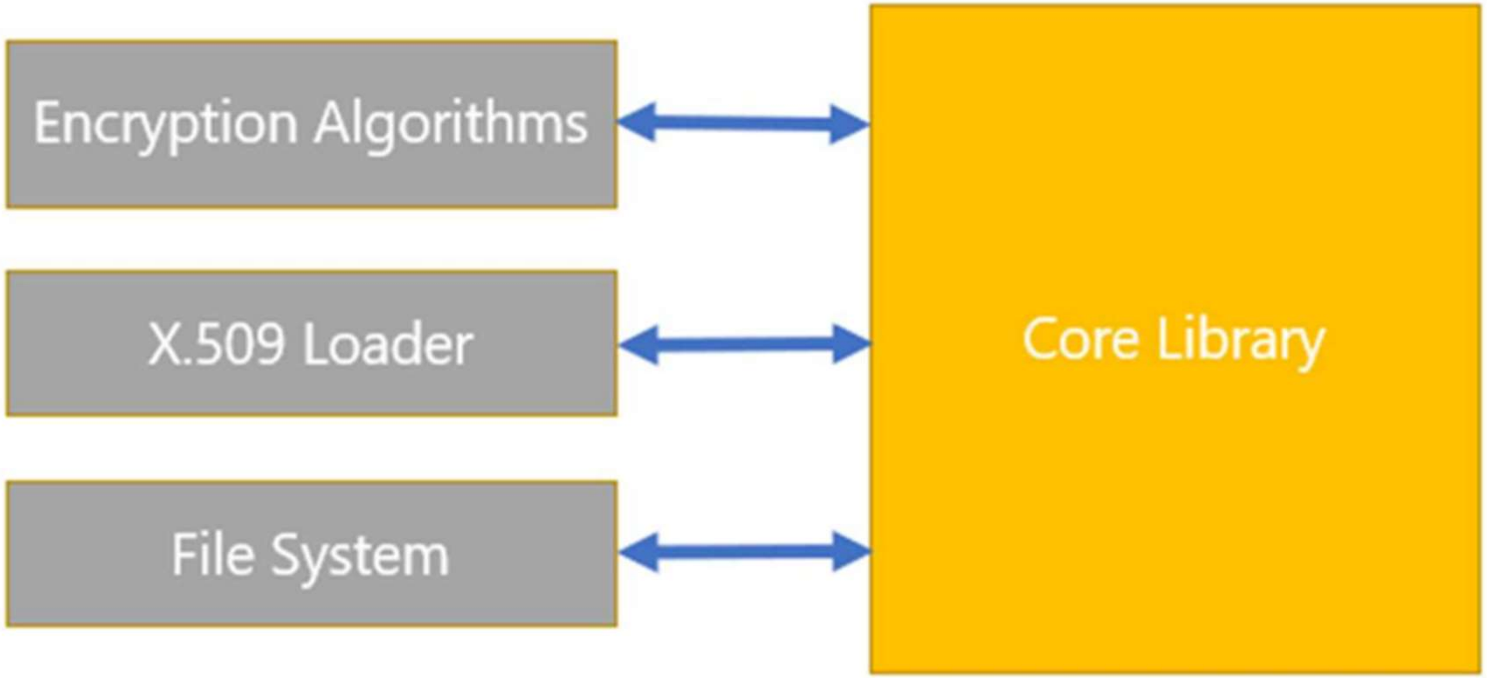


Stories	To Do	In Progress	Testing	Done
Task #1	Task #2 Task #3 Task #6	Task #7 Task #9	Task #8	Task #16 Task 17
New task	Task #10 Task #11	Task #12	Task #13 Task #14	Task #15

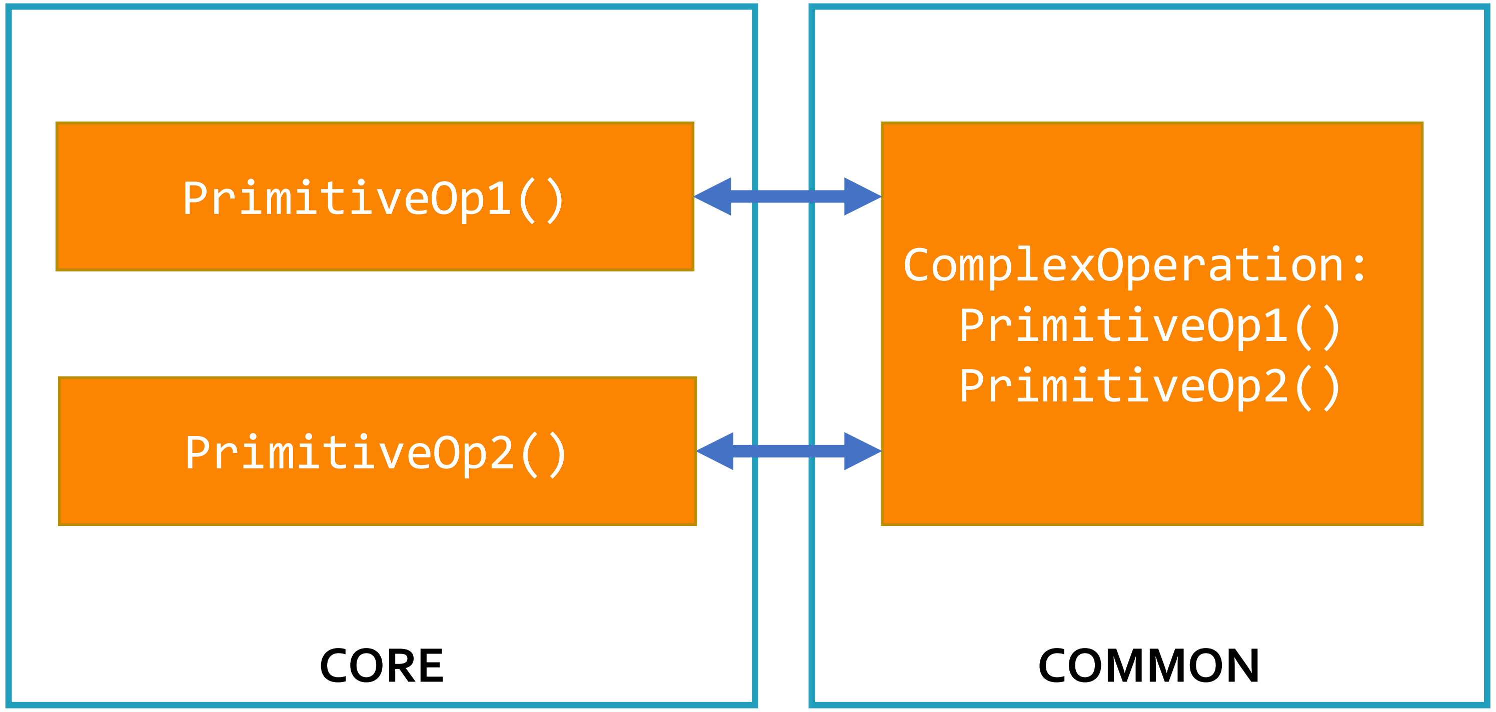
Architecture



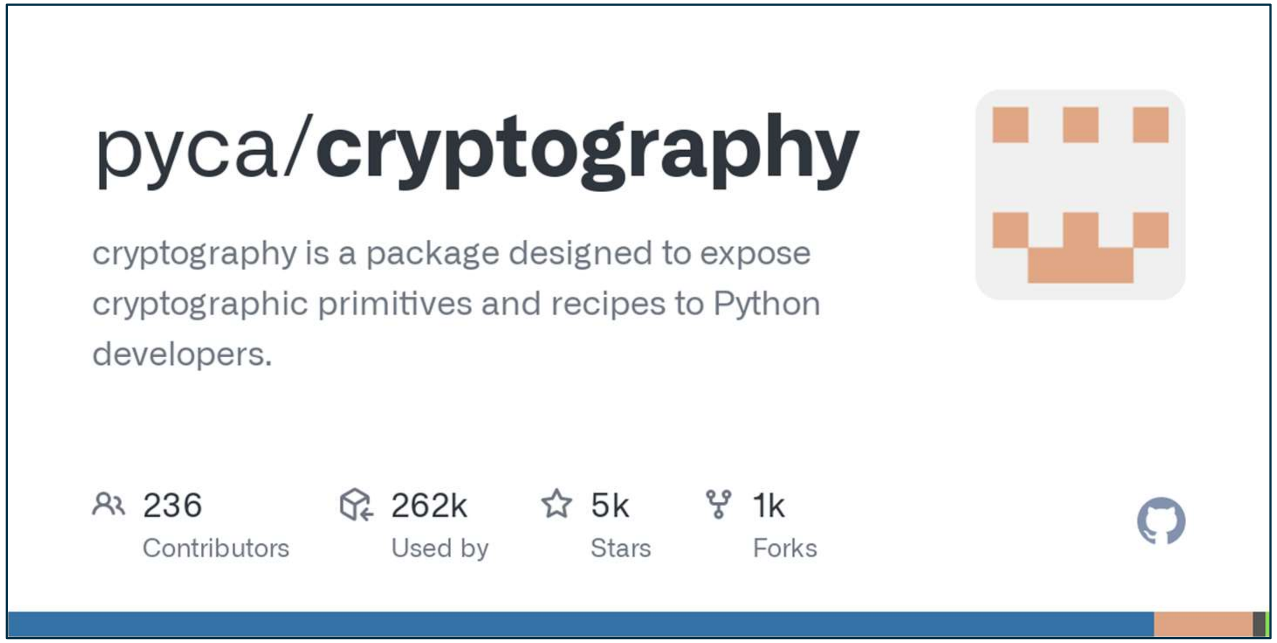
Core Libraries



Common Modules



Implementation



pyca/**cryptography**

cryptography is a package designed to expose cryptographic primitives and recipes to Python developers.

236 Contributors

262k Used by

5k Stars

1k Forks

- Encryption Algorithms
- X.509 Loader & Unloader

Implementation

```
program.py -x arg1 -y arg2
```

- Parses Command Line Arguments

```
program.py −x arg1 −y arg2
```

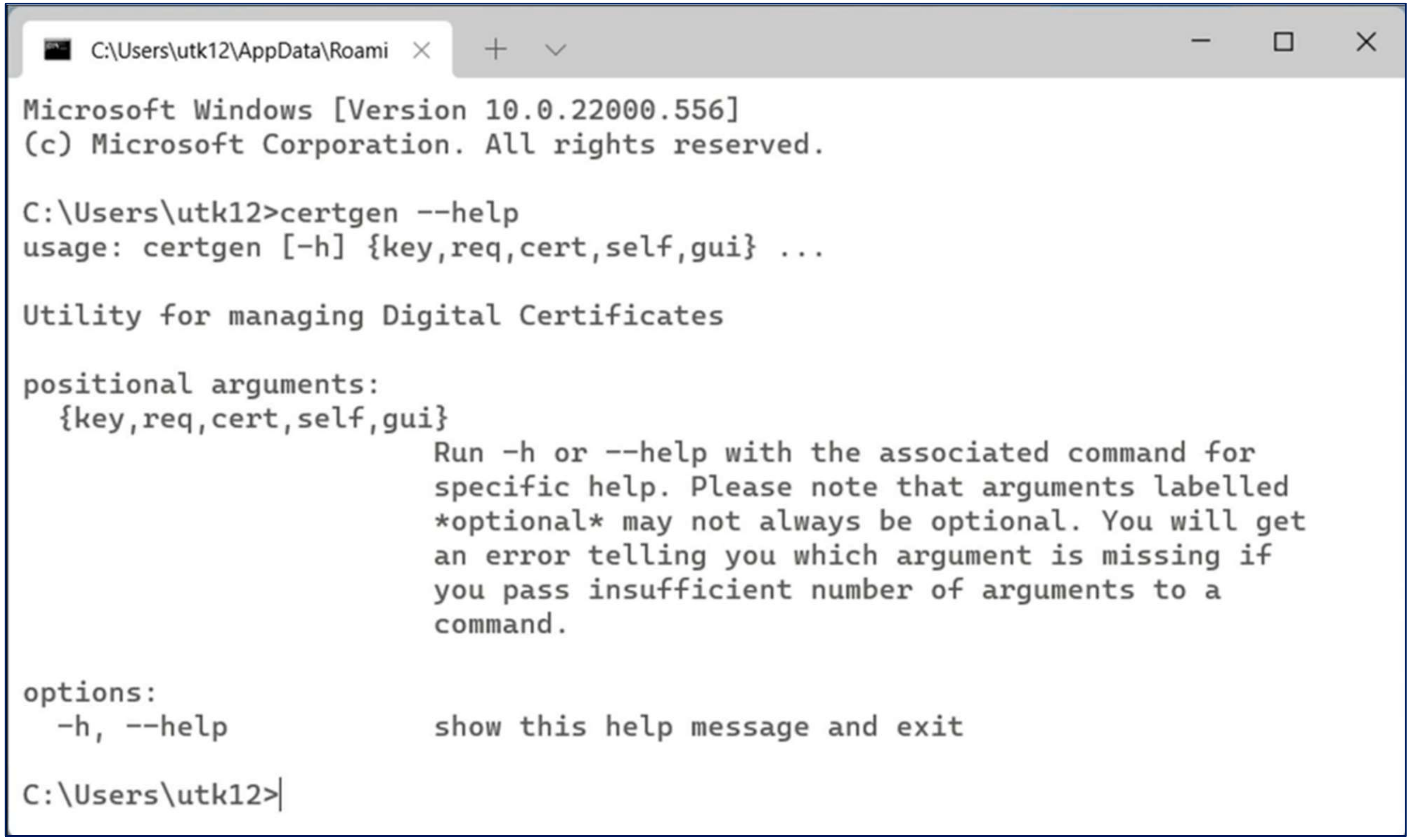
↓

```
args = {
     “x”: “arg1”,
     “y”: “arg2”
}
```

Implementation

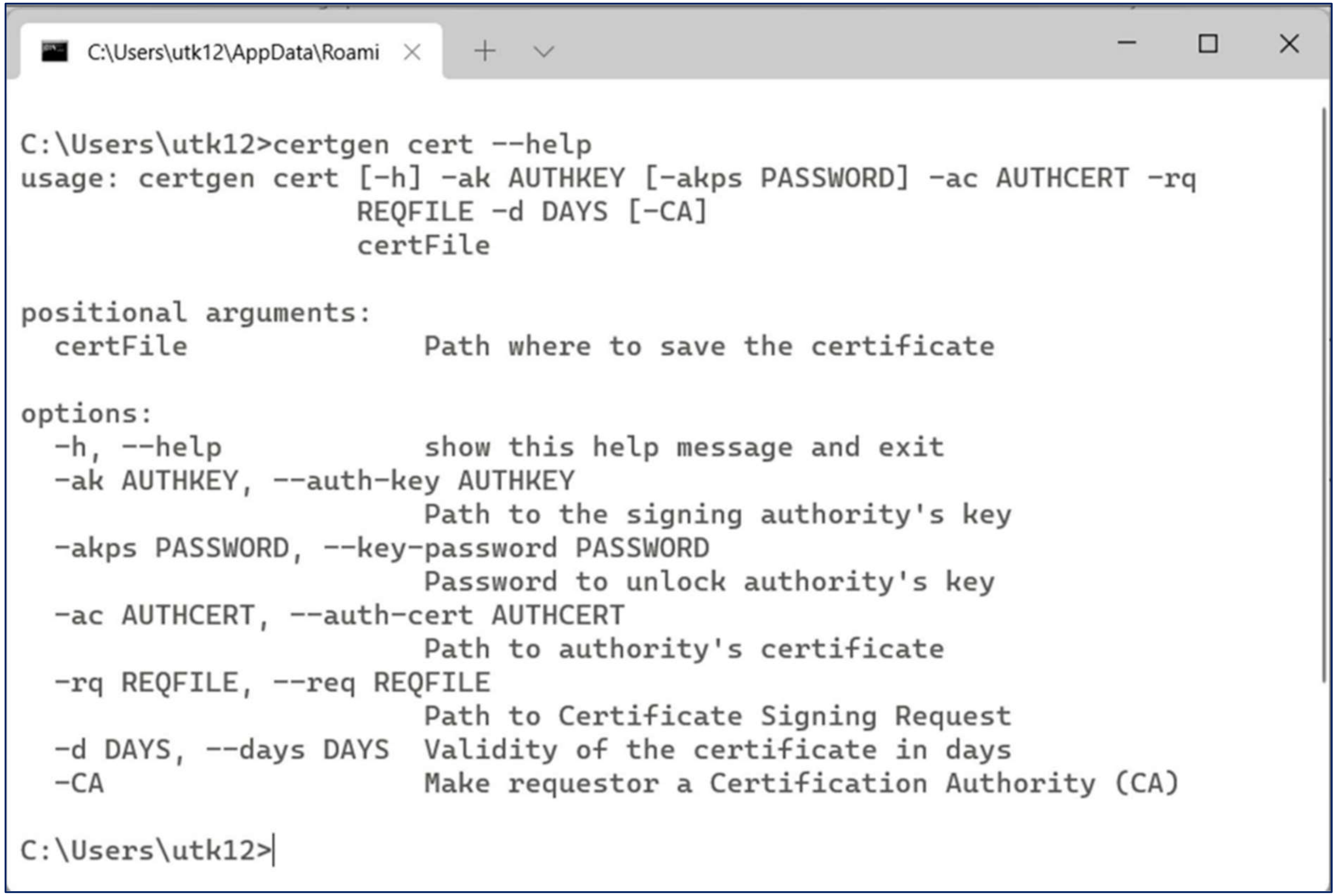
- Cross-platform graphics library
- Separates UI from behavior
- Both UI and behavior written in python

Command-Line Interface



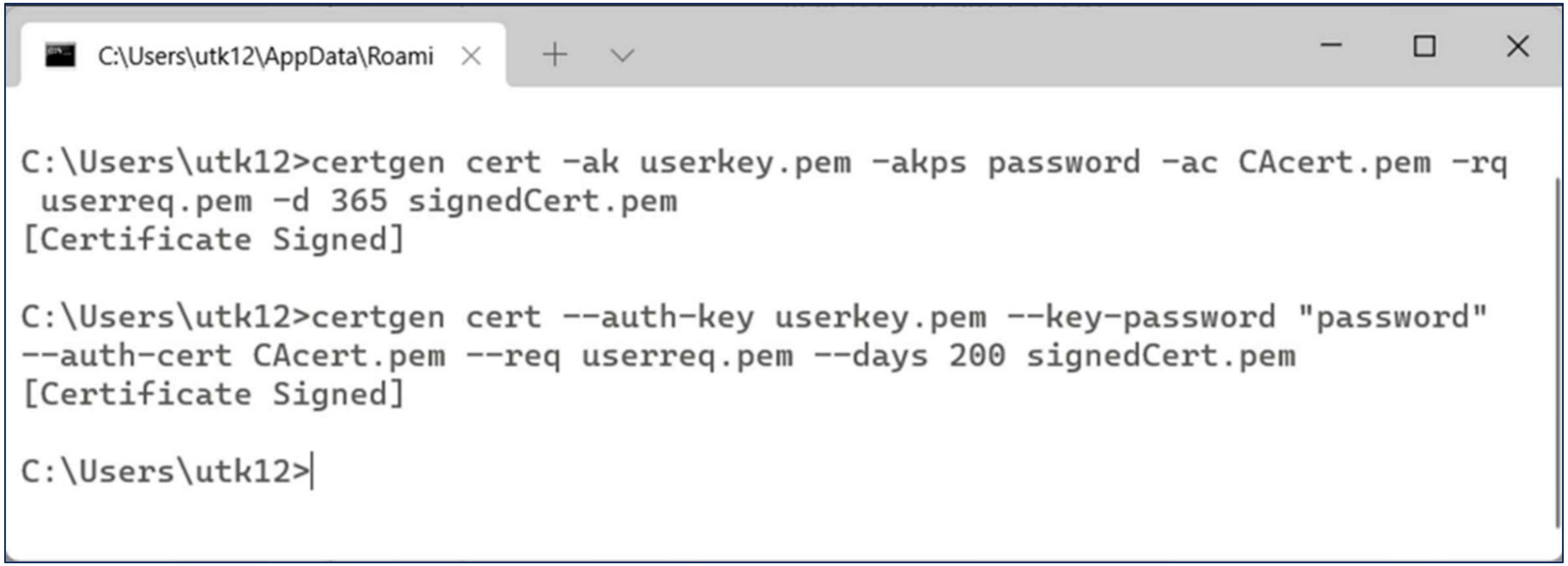
```
Microsoft Windows [Version 10.0.22000.556]
(c) Microsoft Corporation. All rights reserved.

C:\Users\utk12>certgen --help
usage: certgen [-h] {key,req,cert,self,gui} ...

Utility for managing Digital Certificates

positional arguments:
  {key,req,cert,self,gui}
                        Run -h or --help with the associated command for
                        specific help. Please note that arguments labelled
                        *optional* may not always be optional. You will get
                        an error telling you which argument is missing if
                        you pass insufficient number of arguments to a
                        command.

options:
  -h, --help            show this help message and exit

C:\Users\utk12>
```

Command-Line Interface



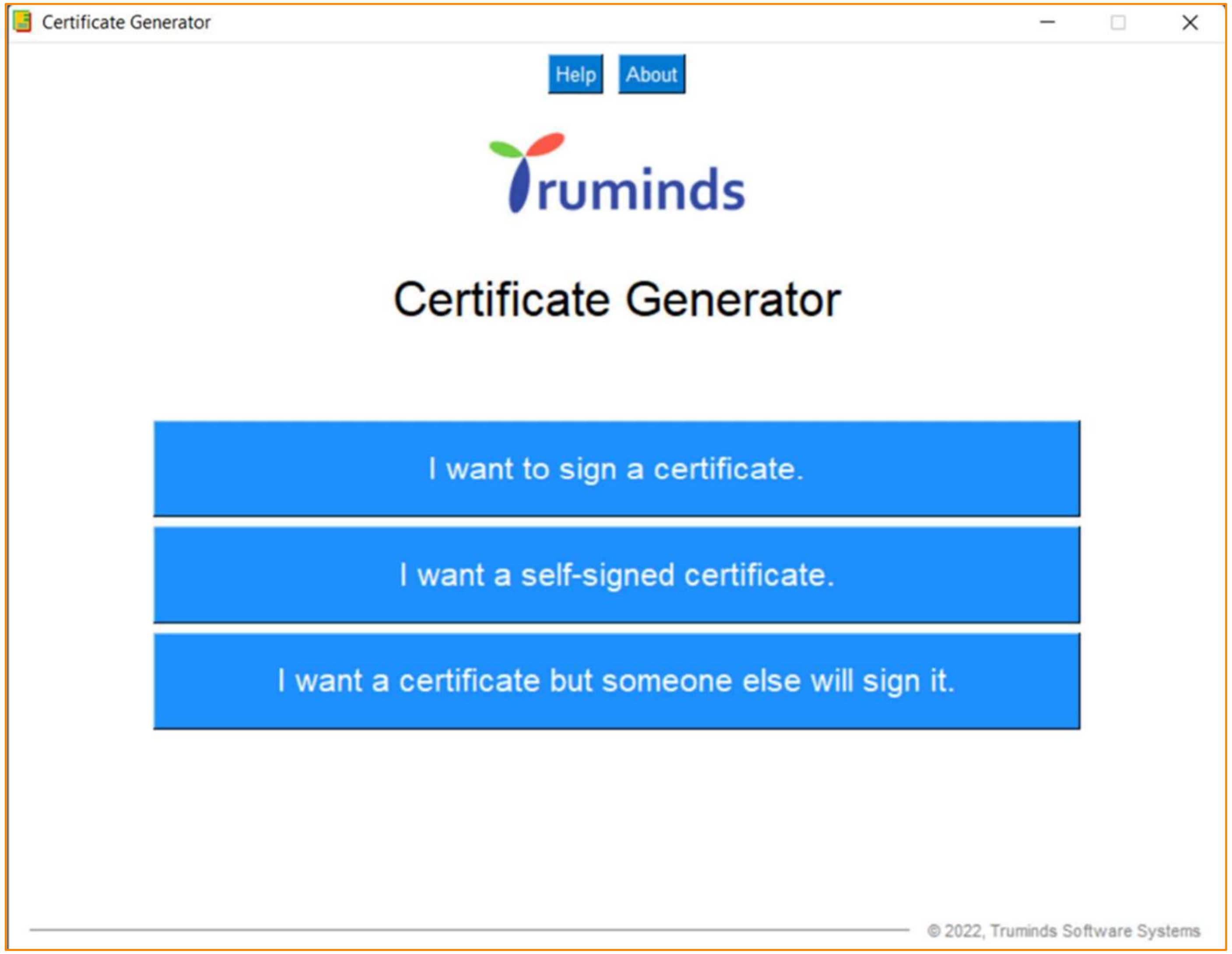
```
C:\Users\utk12>certgen cert --help
usage: certgen cert [-h] -ak AUTHKEY [-akps PASSWORD] -ac AUTHCERT -rq
                    REQFILE -d DAYS [-CA]
                    certFile

positional arguments:
  certFile              Path where to save the certificate

options:
  -h, --help            show this help message and exit
  -ak AUTHKEY, --auth-key AUTHKEY
                        Path to the signing authority's key
  -akps PASSWORD, --key-password PASSWORD
                        Password to unlock authority's key
  -ac AUTHCERT, --auth-cert AUTHCERT
                        Path to authority's certificate
  -rq REQFILE, --req REQFILE
                        Path to Certificate Signing Request
  -d DAYS, --days DAYS  Validity of the certificate in days
  -CA                   Make requestor a Certification Authority (CA)

C:\Users\utk12>
```

Command-Line Interface



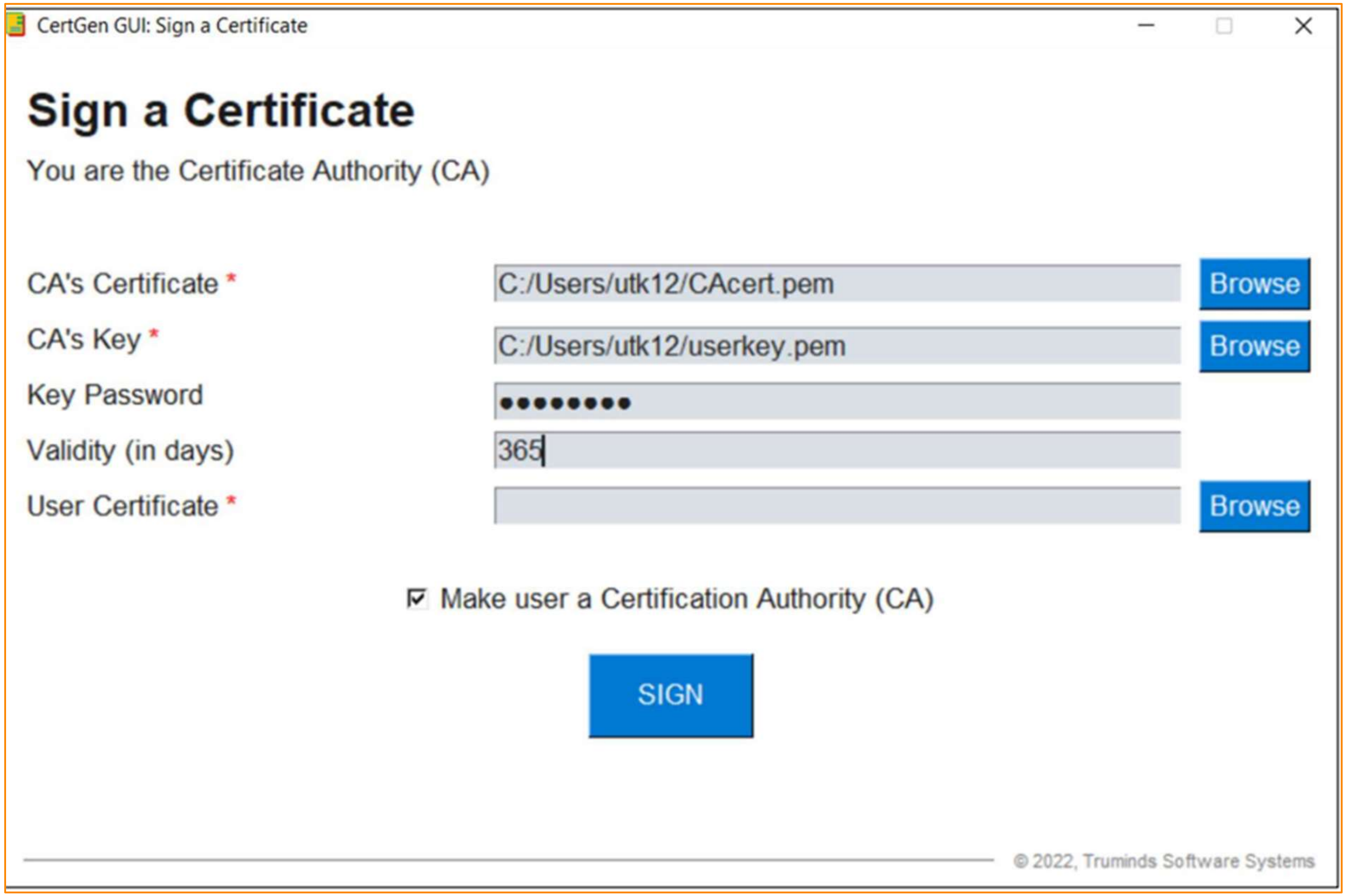
```
C:\Users\utk12>certgen cert -ak userkey.pem -akps password -ac CAcert.pem -rq
 userreq.pem -d 365 signedCert.pem
[Certificate Signed]

C:\Users\utk12>certgen cert --auth-key userkey.pem --key-password "password"
--auth-cert CAcert.pem --req userreq.pem --days 200 signedCert.pem
[Certificate Signed]

C:\Users\utk12>
```

Graphical User Interface



Certificate Generator
Help
About
Truminds
Certificate Generator
I want to sign a certificate.
I want a self-signed certificate.
I want a certificate but someone else will sign it.
© 2022, Truminds Software Systems

Graphical User Interface



CertGen GUI: Sign a Certificate

Sign a Certificate

You are the Certificate Authority (CA)

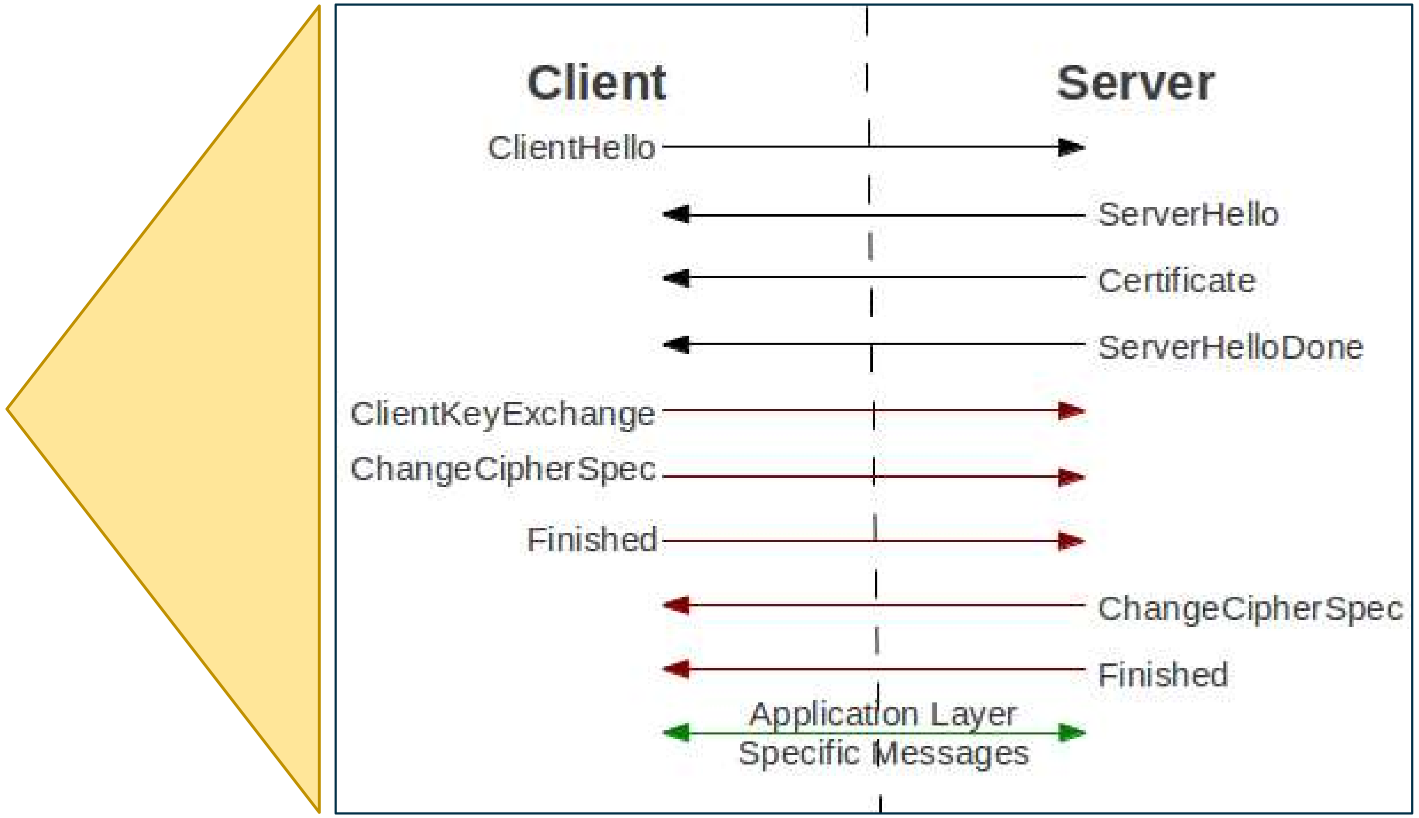
CA's Certificate *	C:/Users/utk12/CAcert.pem
CA's Key *	C:/Users/utk12/userkey.pem
Key Password	●●●●●●●●●
Validity (in days)	365
User Certificate *	

☑ Make user a Certification Authority (CA)

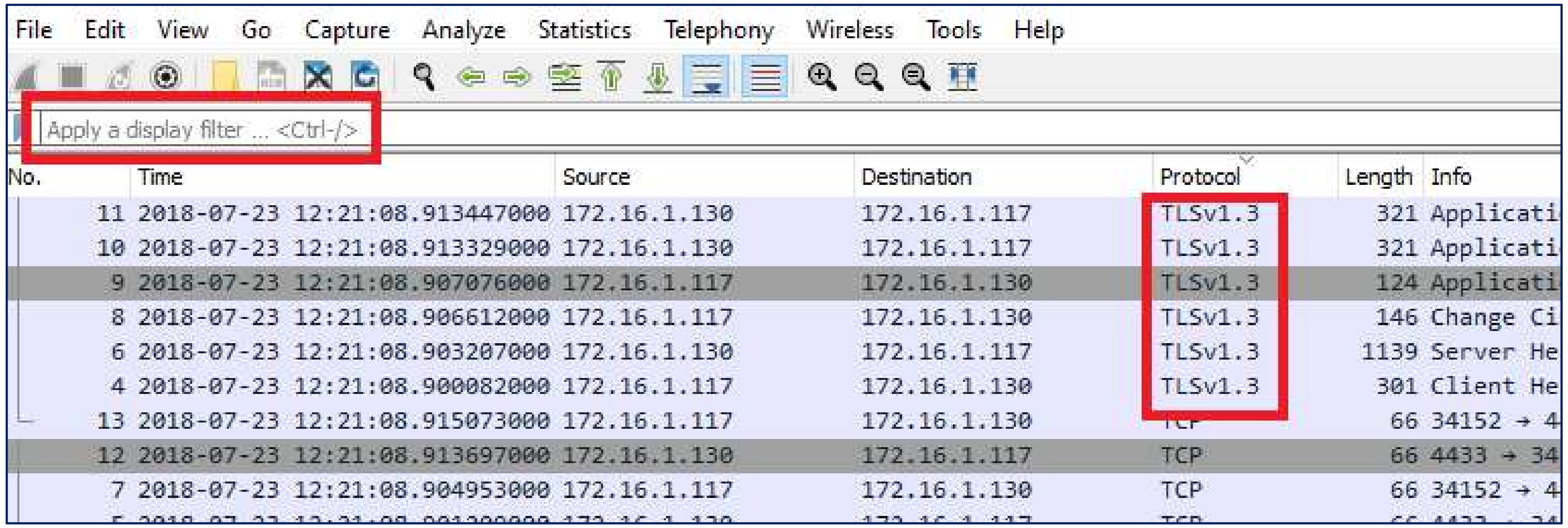
© 2022, Truminds Software Systems

Is our program producing valid certificates?

TLS



Is our program producing valid certificates?



```
No.     Time                           Source         Destination    Protocol   Length  Info
     11 2018-07-23 12:21:08.913447000 172.16.1.130   172.16.1.117   TLSv1.3       321  Applicati
     10 2018-07-23 12:21:08.913329000 172.16.1.130   172.16.1.117   TLSv1.3       321  Applicati
      9 2018-07-23 12:21:08.907076000 172.16.1.117   172.16.1.130   TLSv1.3       124  Applicati
      8 2018-07-23 12:21:08.906612000 172.16.1.117   172.16.1.130   TLSv1.3       146  Change Ci
      6 2018-07-23 12:21:08.903207000 172.16.1.130   172.16.1.117   TLSv1.3      1139  Server He
      4 2018-07-23 12:21:08.900082000 172.16.1.117   172.16.1.130   TLSv1.3       301  Client He
     13 2018-07-23 12:21:08.915073000 172.16.1.117   172.16.1.130   TCP            66  34152 → 4
     12 2018-07-23 12:21:08.913697000 172.16.1.130   172.16.1.117   TCP            66  4433 → 34
      7 2018-07-23 12:21:08.904953000 172.16.1.117   172.16.1.130   TCP            66  34152 → 4
```

Wireshark Capture

Summary

- Concept of Digital Certificates
- Requirements
- Action Plan – Agile Methodology & Progress Tracking
- Architecture
- Implementation
- Results & Features
- Testing

MCA-722

Project Presentation

MAY 2022

Certificate Generator

Utkarsh Gupta (192120009)

Internal Supervisor

Dr. Sanjay Sharma
Professor
Maulana Azad National Institute of Technology
Bhopal

External Supervisor

Mr. Pankaj Choudhary
Senior Technical Lead
Truminds Software Systems
Gurugram