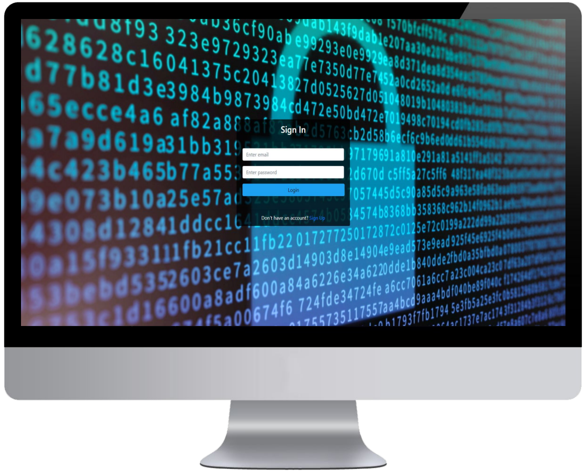
Smartphone as a security token

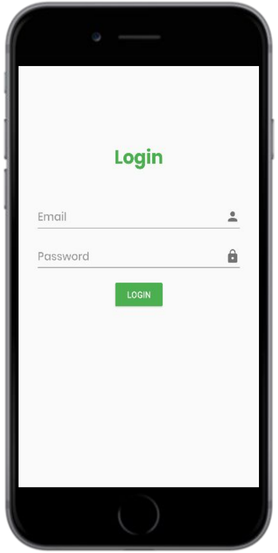
Group 14

Solution

Overview, Requirements, Architecture

Overview

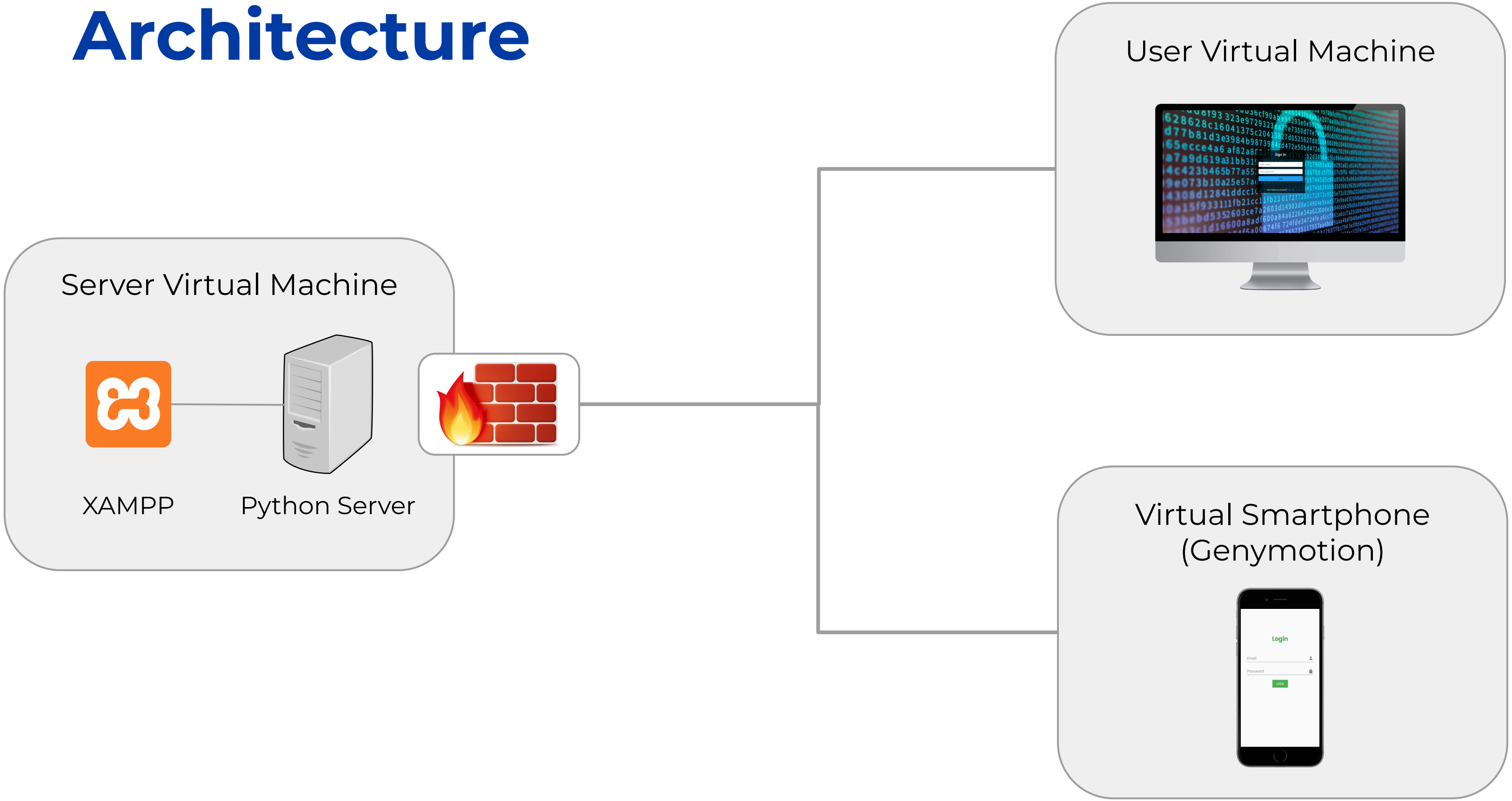

Sign In
Enter email
Enter password
Login
Don't have an account? Sign Up


Login
Email
Password
LOGIN

Solution Requirements

- **Confidentiality:** data must be encrypted;
- **Integrity:** data can’t be tampered with and should be preserved;
- **Authentication:** two-factor authentication;
- **Non-repudiation:** data must be signed;
- **Freshness:** token is valid for short time.

Architecture



Server Virtual Machine

XAMPP

Python Server

User Virtual Machine

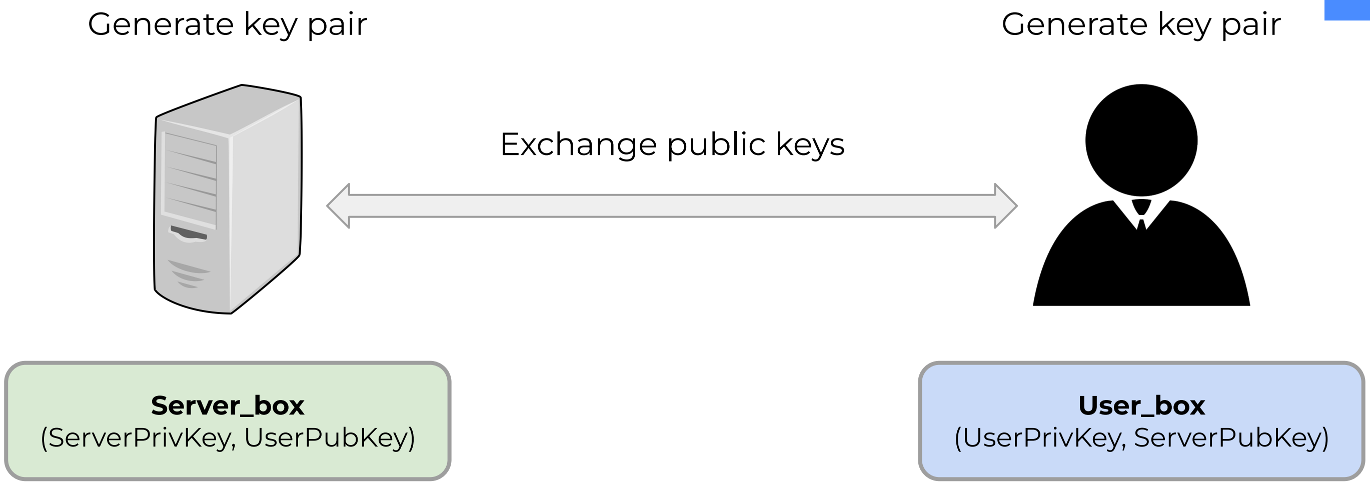
Virtual Smartphone (Genymotion)

Keys

Encryption keys, Digital signature

Encryption Keys

- **Curve25519** (efficient and secure);
- Ensures **confidentiality** and **integrity.**



Generate key pair

Generate key pair

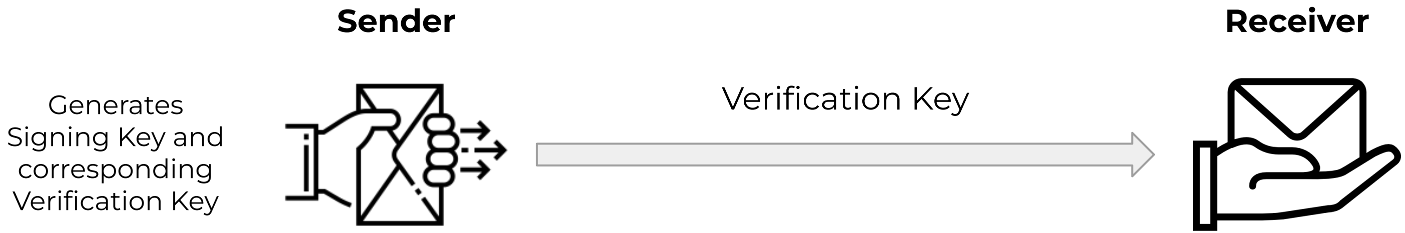
Exchange public keys

Server_box
(ServerPrivKey, UserPubKey)

User_box
(UserPrivKey, ServerPubKey)

Signing Keys (digital signatures)

- **Ed25519** (high security and fast signing, key generation and batch verification);
- Ensures **authenticity, non-repudiation** and **integrity.**



Sender

Receiver

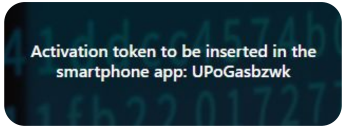
Generates Signing Key and corresponding Verification Key

Verification Key

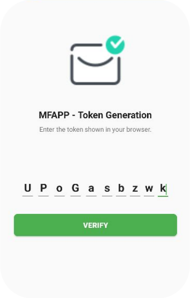
Protocols

Register and Login protocols

Register Protocol



Activation token to be inserted in the smartphone app: UPoGasbzwk

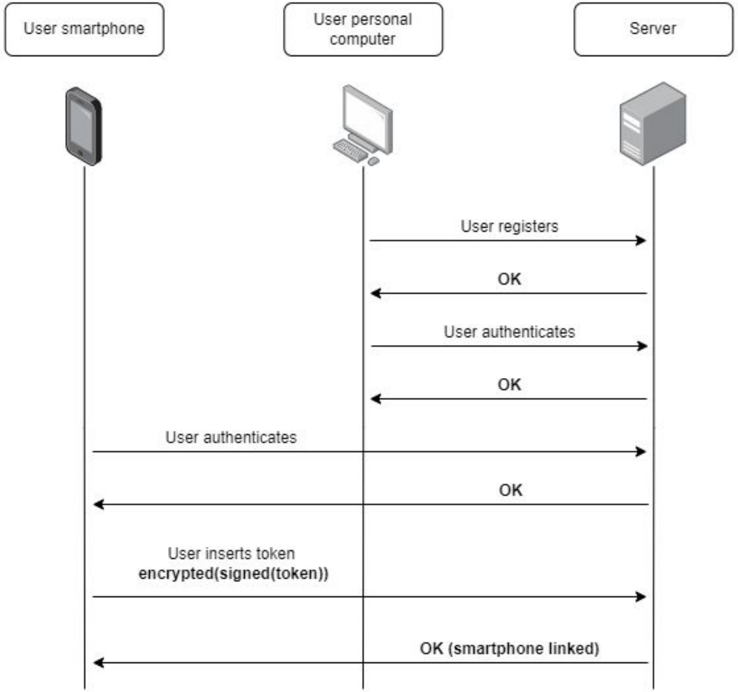


MFAPP - Token Generation

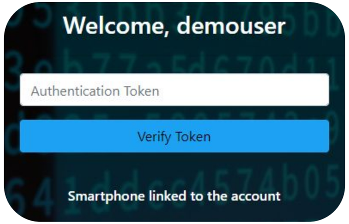
Enter the token shown in your browser.

UPoGasbzwk

Token being inserted in the smartphone application (unique token)

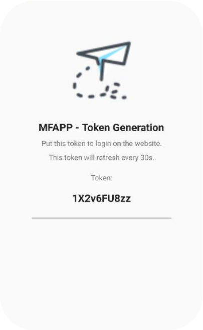


Login Protocol



Welcome, demouser

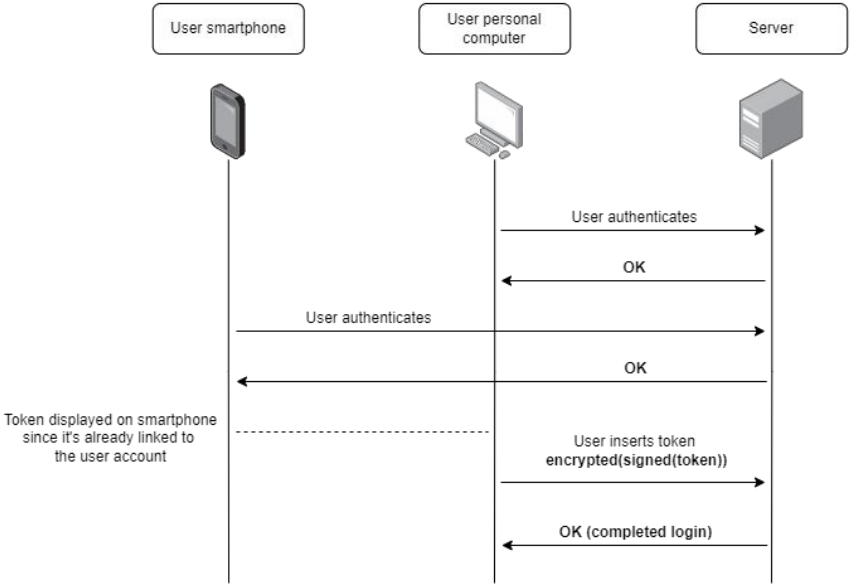
Smartphone linked to the account


MFAPP - Token Generation

Put this token to login on the website.
This token will refresh every 30s.

Token:
1X2v6FU8zz

Token to insert in the web application so the user can fully login (unique token)


User smartphone

User personal computer

Server

User authenticates

OK

User authenticates

OK

Token displayed on smartphone since it's already linked to the user account

User inserts token
encrypted(signed(token))

OK (completed login)

Demo

Video demonstration

Video demonstration 2