NUSMED

A NHC Parody

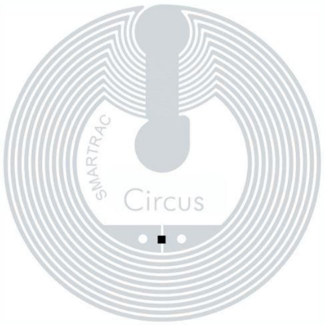
Prototype Presentation

IFS4205 Team 02

AY19/20

NUSMED
A NHC Parody

System Summary



Token ID

Device ID

NRIC and Password

Authentication

- Web Server
  - Use of **Form Authentication** to hold authenticated sessions.
  - **ASP.NET Membership** is used to authorize roles to specific directories.

- Android Application
  - Use of NRIC + password + mobile device + NFC tag to authenticate
  - JSON Web Token (**JWT**)
  - Web server caches JWT token to maintain sessions

Account Roles

Account Roles

- Patient
- Therapist
- Researcher
- Administrator (Clerk, Nurse, etc)

Accounts are able to possess multiple roles at the same time, but user can only log in as one role each time.

Permission System

Relevant for Patient Information and Records.

- Record Types
  - Therapists requests for and Patients approves. (whitelisting)
- Fine-Grain Record Permissions
  - To blacklist specific therapists from certain records.
- Global Record Permissions
  - To “delete” records.

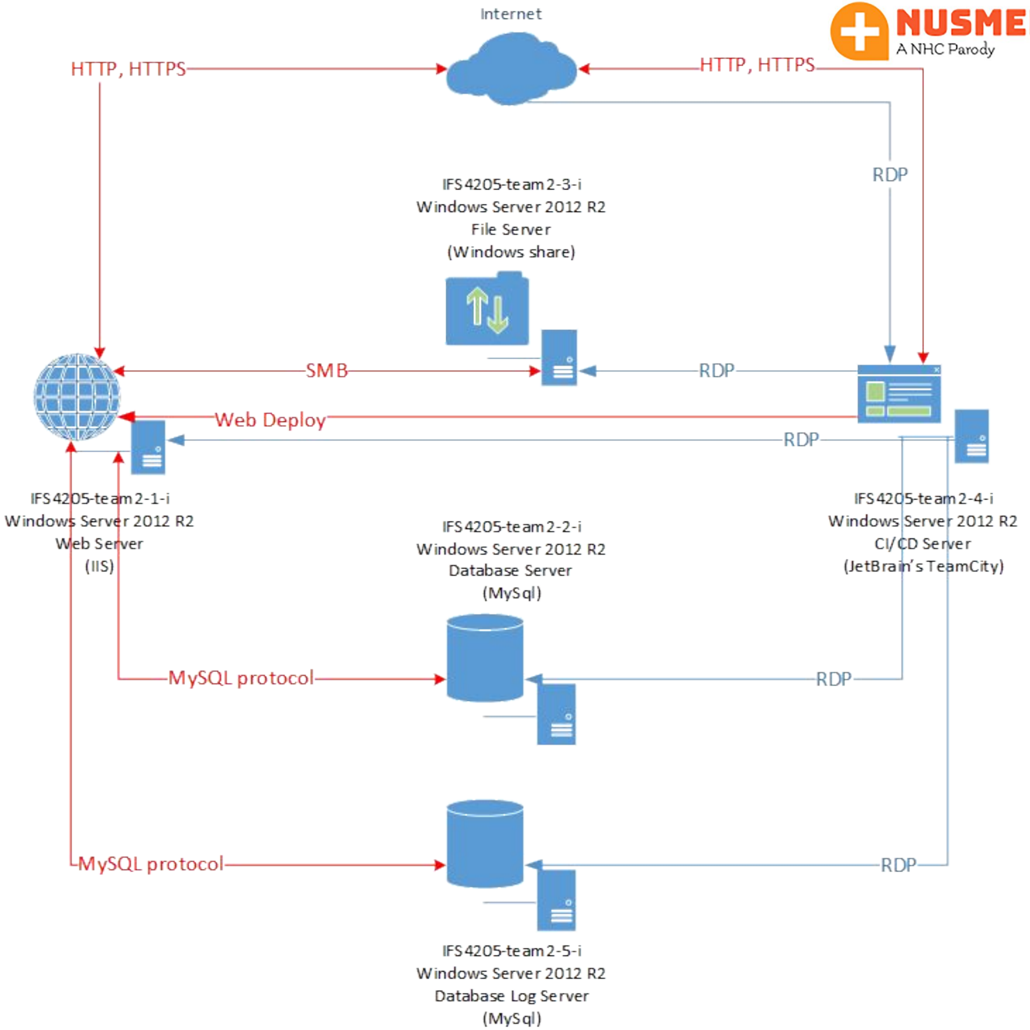
Patient information can be viewed by only approved therapists.

K-Anonymisation

- Datafly algorithm
- Quasi-identifiers: Age, Sex, Gender, Marital Status, Postal Code, Record Creation Date
- K: 3
- Suppression threshold: 5%

System Architecture

- 1x CI/CD and Jump Host machine
  - Web Deploy
- 2x Database Server
  - Remote to Web Server only (TLS1.2)
- 1x File Server
  - Authentication via AD (SMB 3.1.1)
  - Todo: File screening and whitelisting
- 1x Web Server
  - IIS configured for TLS1.3



NUSMED
A NHC Parody

-System Demo-

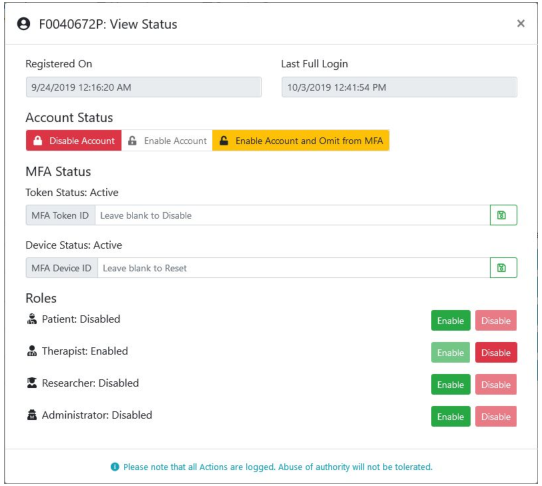
-Security Claims-

K-Anonymisation

- Datafly algorithm
- Quasi-identifiers: Age, Sex, Gender, Marital Status, Postal Code, Record Creation Date
- K: 3
- Suppression threshold: 5%

Registration

Admin assigns token



F0040672P: View Status ×

Registered On: 9/24/2019 12:16:20 AM

Last Full Login: 10/3/2019 12:41:54 PM

Account Status

Disable Account | Enable Account | Enable Account and Omit from MFA

MFA Status

Token Status: Active

MFA Token ID: Leave blank to Disable

Device Status: Active

MFA Device ID: Leave blank to Reset

Roles

Patient: Disabled — Enable | Disable

Therapist: Enabled — Enable | Disable

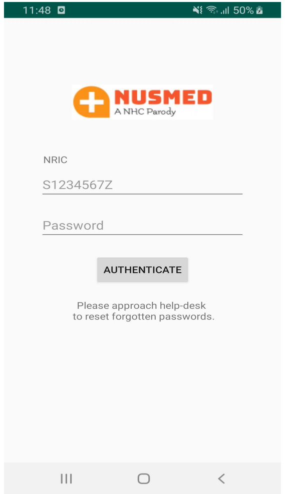
Researcher: Disabled — Enable | Disable

Administrator: Disabled — Enable | Disable

Please note that all Actions are logged. Abuse of authority will not be tolerated.

- Token ID is a 128-bit UUID generated by java.util.UUID library
- Admin manually assigns a token to a user via admin console

User authenticates with registered credentials and issued token

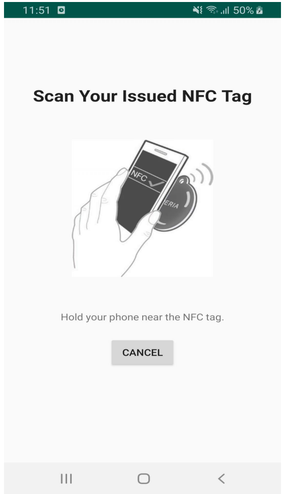


NRIC: S1234567Z

Password

AUTHENTICATE

Please approach help-desk to reset forgotten passwords.



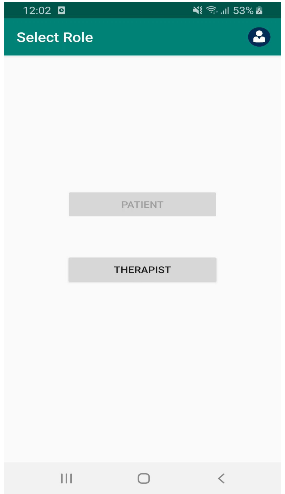
Scan Your Issued NFC Tag

Hold your phone near the NFC tag.

CANCEL

- User downloads app which automatically generates a 128-bit device ID via the java.util.UUID library upon launch
- The device ID would be tagged to the user thus scanning the token from another phone would not work

User selects role



Select Role

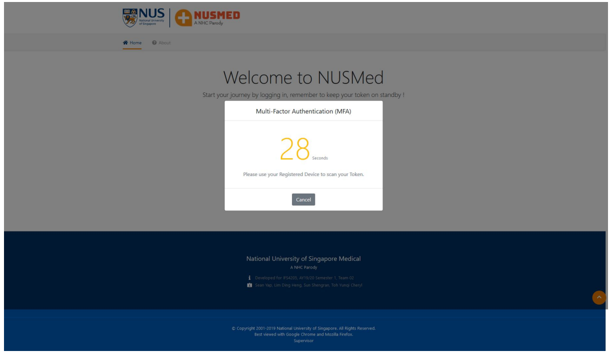
PATIENT

THERAPIST

- User is able to select only the roles he has
- App is assigned a JWT which expires after 15 mins of inactivity

Web Login

User logs in on web app



Welcome to NUSMed

Start your journey by logging in, remember to keep your token on standby !

Multi-Factor Authentication (MFA)

28 Seconds

Please use your Registered Device to scan your Token.

National University of Singapore Medical

A NHC Parody

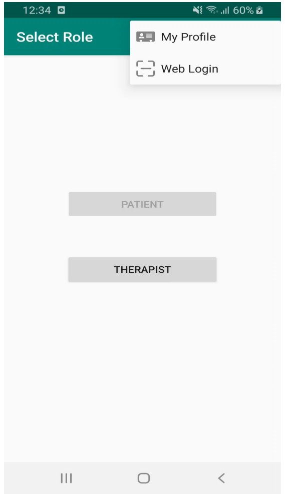
Developed for IFS4205, AY19/20 Semester 1, Team 02

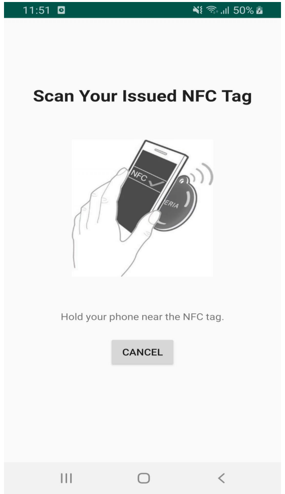
Sean Yap, Lim Ding Heng, Sun Shengran, Toh Yunqi Cheryl

© Copyright 2001-2019 National University of Singapore. All Rights Reserved.
Best viewed with Google Chrome and Mozilla Firefox.
Supervisor

- User has 30 seconds to scan his issued NFC token via the mobile application

User selects web login on the mobile application





Scan Your Issued NFC Tag

Hold your phone near the NFC tag.

- App would send the device ID, token ID and the JWT to the server to be validated