User Access to Health Information Systems with W3C Verifiable Credentials

David W Chadwick
University of Kent

Acknowledgements

This work was performed in collaboration with

Romain Laborde, Samer Wazan, Arnaud Oglaza
IRIT Laboratory, Paul Sabatier University, France

And

Declan Barnes
University of Kent

And

Dr Manreet Nijjar
Truu ltd (previously Doctors Link Ltd)

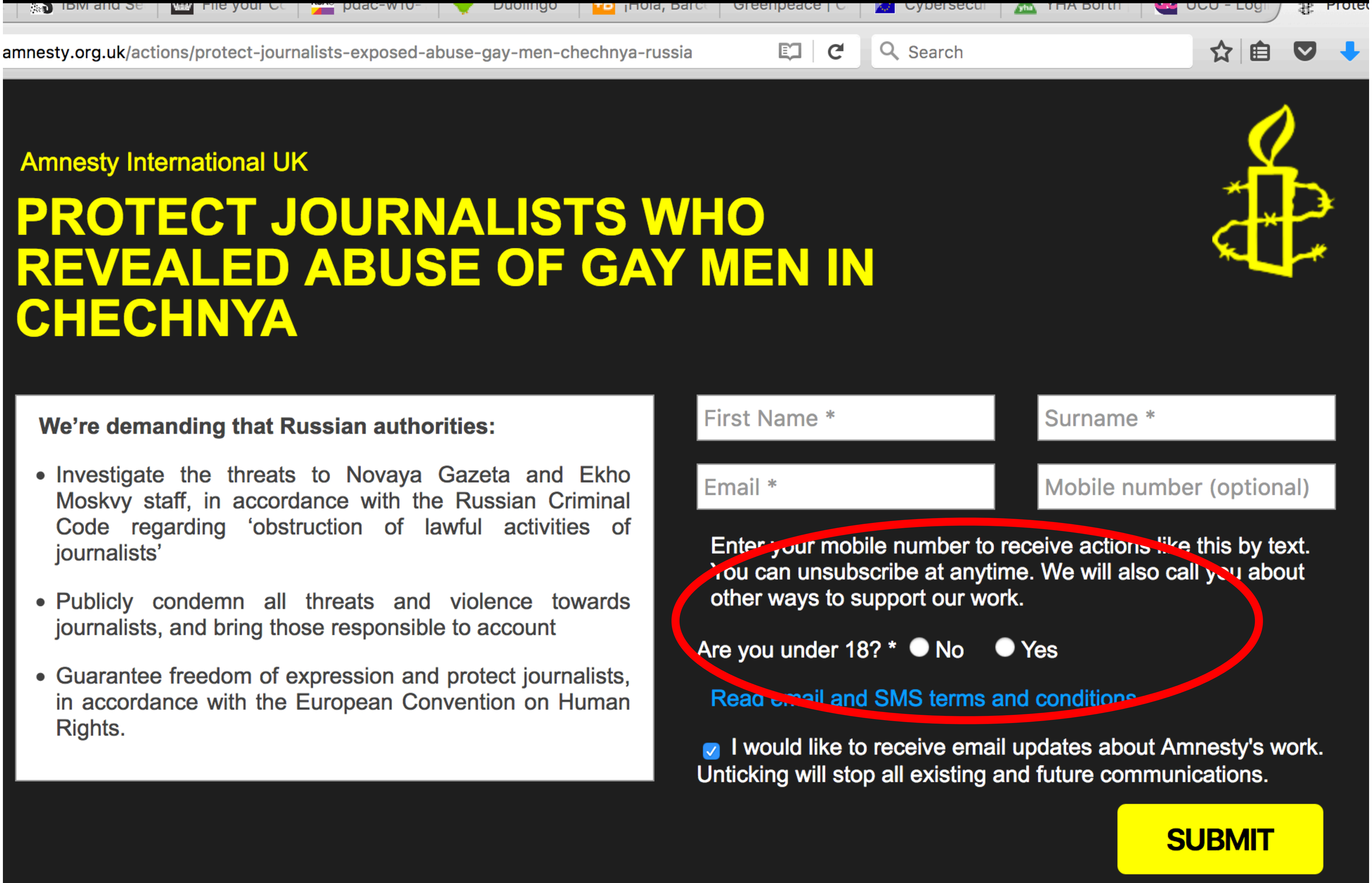
What are Verifiable Credentials?

- Potentially long-lived electronic credentials that the user stores under his/her control and uses as he/she wishes in order to access electronic resources
- Contain certified identity attributes (PII)
- Used as Authorisation tokens in ABAC systems

Why are VCs needed?

- Because most web sites today are not able to verify a user's identity attributes
  - They either trust the user, or do not offer the online service
- Because today's federated identity management infrastructures have a number of limitations that VCs address

Amnesty Petition – Are you under 18?



amnesty.org.uk/actions/protect-journalists-exposed-abuse-gay-men-chechnya-russia

Amnesty International UK

PROTECT JOURNALISTS WHO REVEALED ABUSE OF GAY MEN IN CHECHNYA

We're demanding that Russian authorities:

- Investigate the threats to Novaya Gazeta and Ekho Moskvy staff, in accordance with the Russian Criminal Code regarding 'obstruction of lawful activities of journalists'
- Publicly condemn all threats and violence towards journalists, and bring those responsible to account
- Guarantee freedom of expression and protect journalists, in accordance with the European Convention on Human Rights.

First Name *

Surname *

Email *

Mobile number (optional)

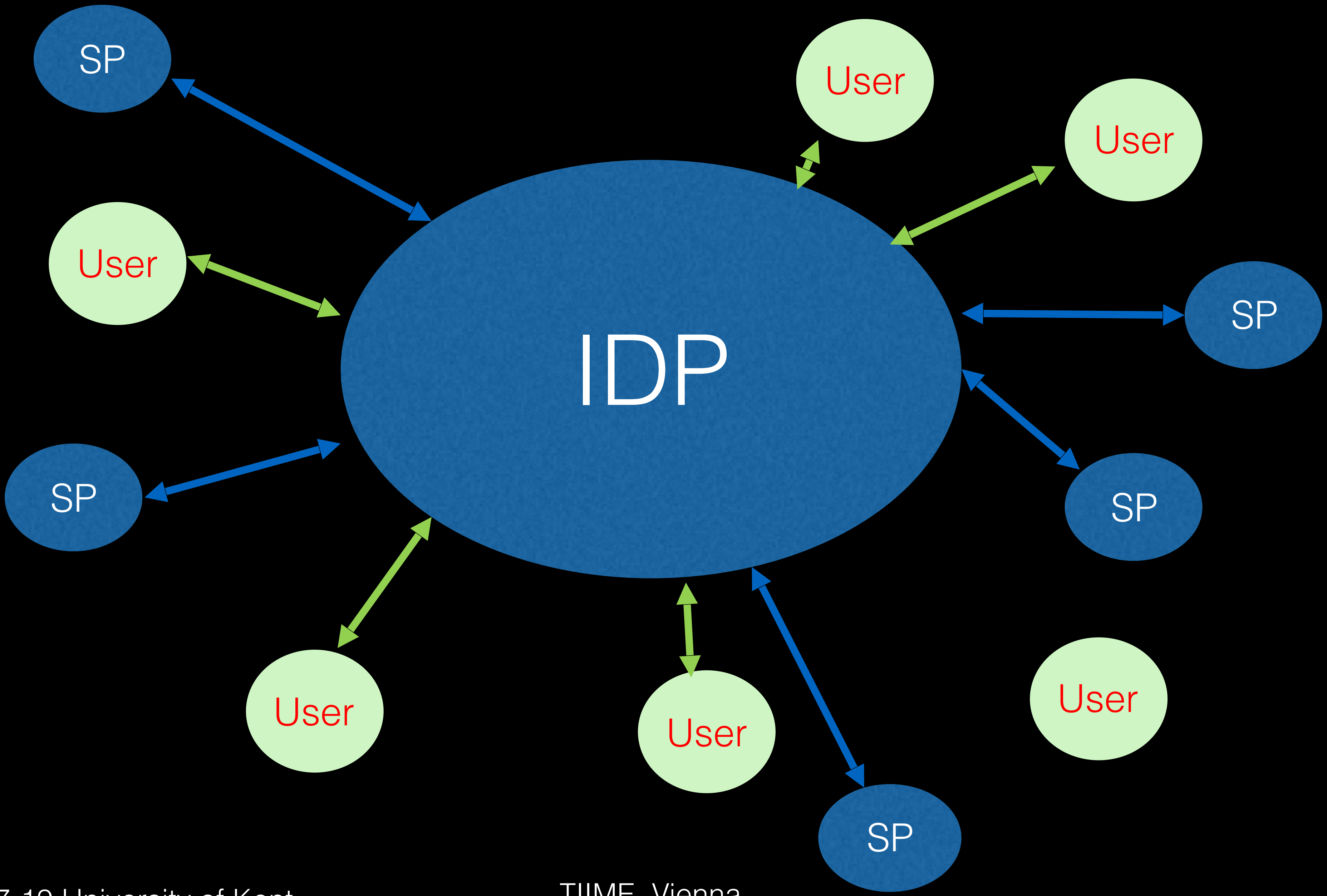
Enter your mobile number to receive actions like this by text. You can unsubscribe at anytime. We will also call you about other ways to support our work.

Are you under 18? * ○ No ○ Yes

Read email and SMS terms and conditions

☑ I would like to receive email updates about Amnesty's work. Unticking will stop all existing and future communications.

FIM Limitations



FIM Limitations

- "Insufficient attribute release by IdPs is considered by user communities as the major problem today in the eduGAIN space" [1].

[1] EU AARC Project Deliverable DNA2.4 "Training Material Targeted at Identity Providers" 27 July 2016. Available from https://aarc-project.eu/wp-content/uploads/2016/07/AARC-DNA2.4.pdf

FIM Limitations

- Trust model is wrong: IdPs have to trust SPs to keep user’s attributes private
  - IdPs are often unwilling to release some of the user’s identity attributes to any SP
  - IdPs are not willing to release any of the user’s attributes to most SPs (since they are not in the IdP’s federation)

FIM Limitations

- SPs may require attributes from multiple authorities (Attribute Aggregation)
    - Some do this by assigning a globally unique ID to the user, which provides a privacy invasive correlating handle
- IdP sends all user's attributes at login before service is chosen so does not provide Least Privileges
- Susceptible to phishing attacks by redirection to fraudulent IdP

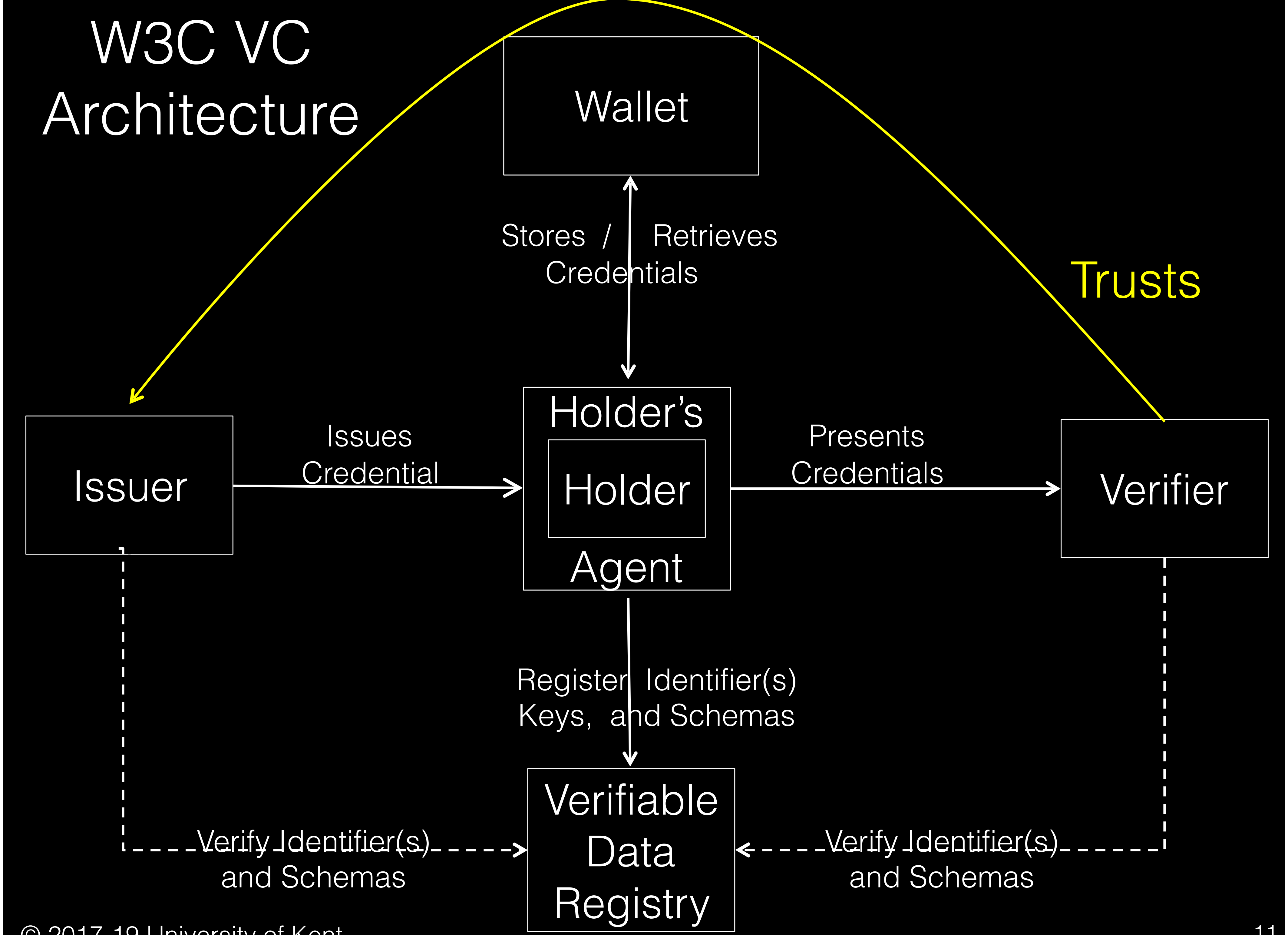
Compare FIM assertions to Plastic Cards, Passports etc.

- Users can show their credentials to any SPs that ask for them, without the issuer being aware of this, or able to stop it
- Users can aggregate these credentials as required by the SPs
- Users can ask issuers to revoke their credentials on demand
- USERS ARE IN CONTROL

➢ Verifiable Credentials are the electronic equivalent of today's physical credentials, only better

  - More secure, more privacy protecting

W3C VC Architecture


Wallet
Stores / Retrieves Credentials
Trusts
Issuer
Issues Credential
Holder's
Holder
Agent
Presents Credentials
Verifier
Register Identifier(s) Keys, and Schemas
Verifiable Data Registry
Verify Identifier(s) and Schemas
Verify Identifier(s) and Schemas

© 2017-19 University of Kent

TIIME, Vienna

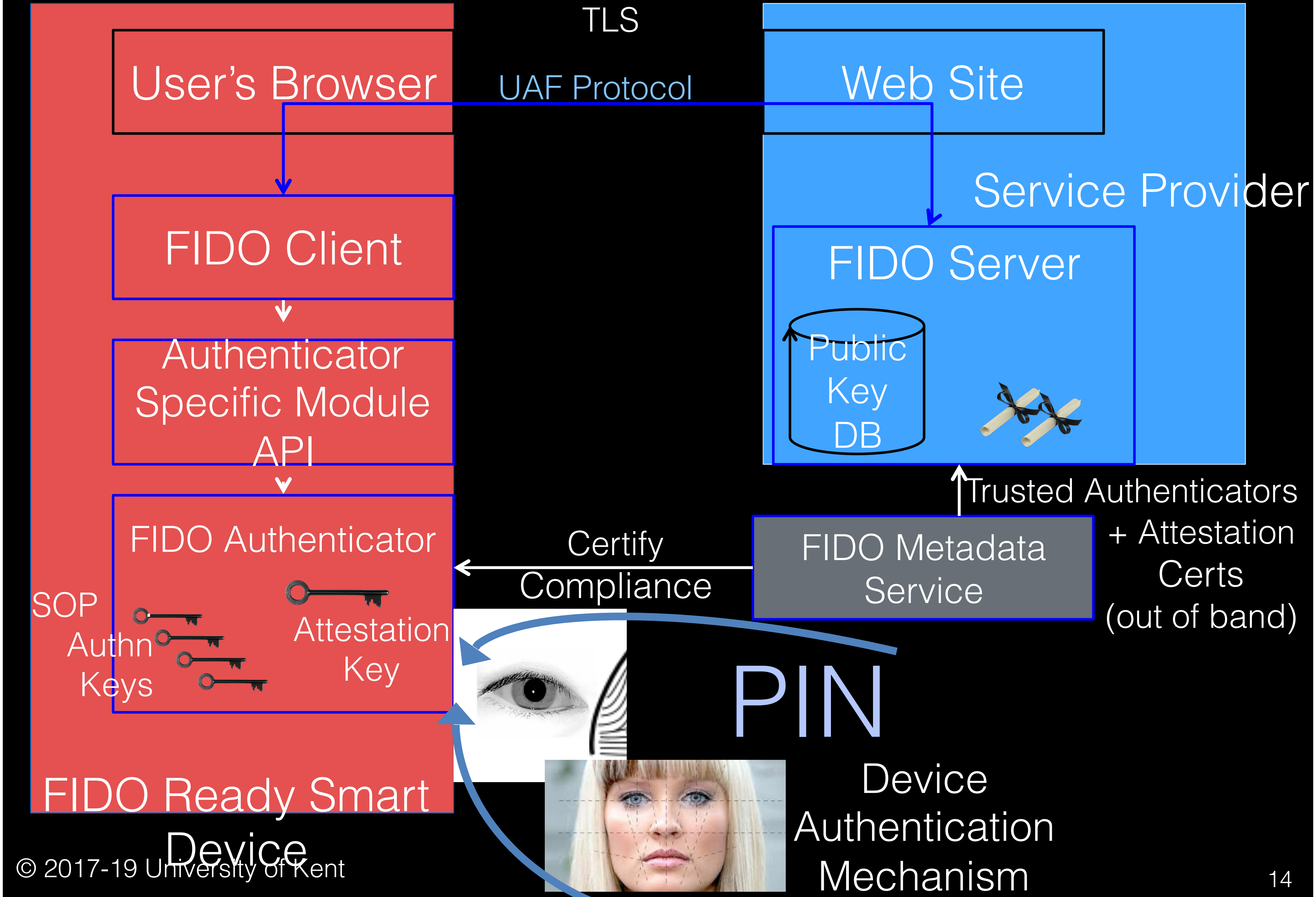
Verifiable Credentials Standardisation

- VC Working Group only tasked with standardizing a data model for VCs
- Protocols are out of scope

Fast Identity Online - FIDO

- The FIDO Alliance developed specifications for strong authentication (and taken to W3C for standardization)
- Uses asymmetric encryption, with a unique key pair created for every web site the user visits
- Two specifications
  - UAF: Universal Authentication Framework for password-less authentication from FIDO enabled smart devices
  - U2F:Universal Second Factor protocol (U2F) for two factor authentication using a small hardware token to accompany a non-FIDO smart device having a FIDO compliant web browser

FIDO UAF Architecture



TLS

User's Browser

UAF Protocol

Web Site

Service Provider

FIDO Client

FIDO Server

Public Key DB

Authenticator Specific Module API

FIDO Authenticator

Trusted Authenticators + Attestation Certs (out of band)

Certify Compliance

FIDO Metadata Service

SOP Authn Keys

Attestation Key

PIN

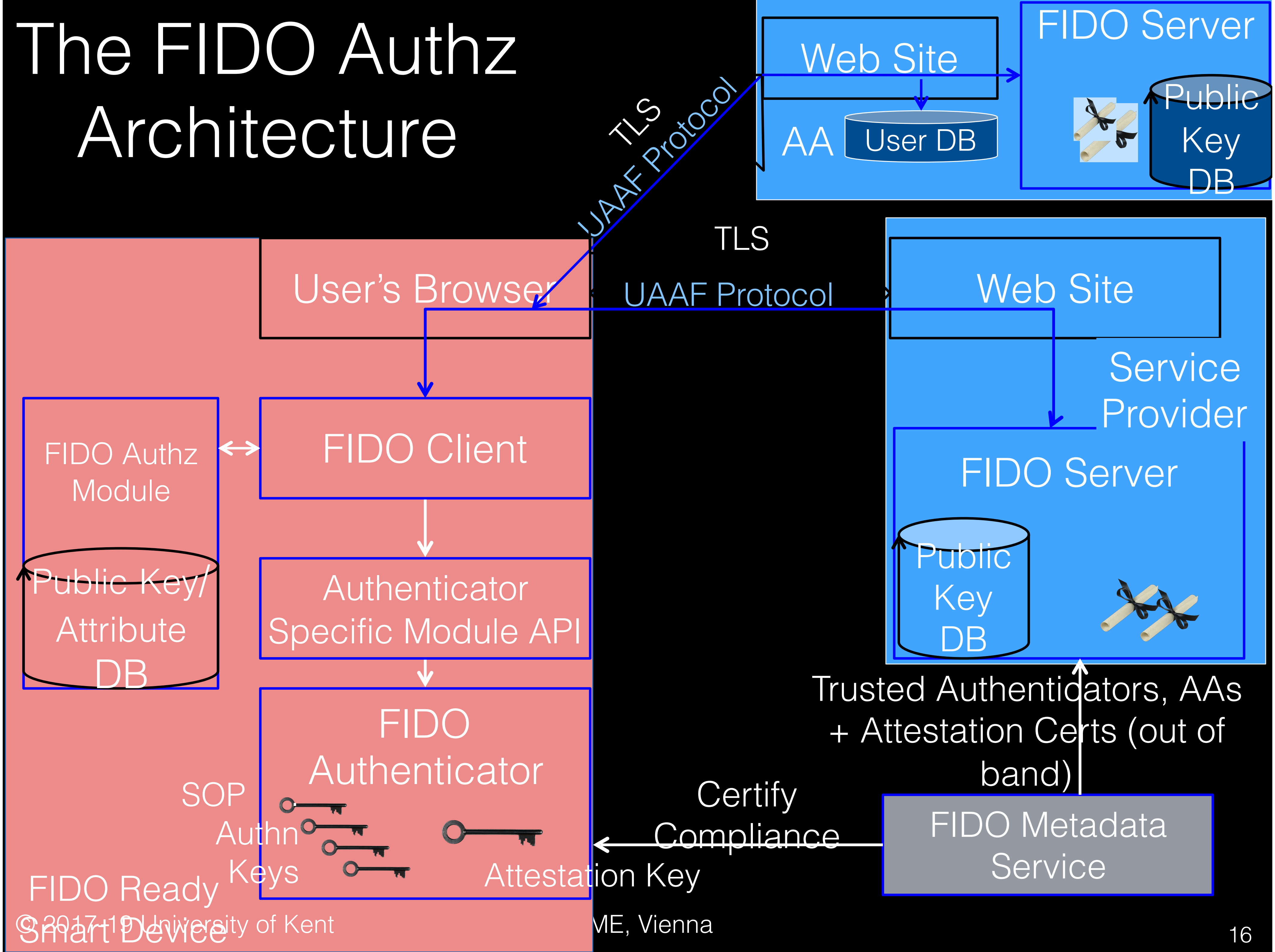
FIDO Ready Smart Device

Device Authentication Mechanism

BUT…

- FIDO only provides strong authentication
- It does not identify the user
- It does not provide authorisation
    - which are the main goals of verifiable credentials
- So… we devised an authorisation enhancement for FIDO, that conforms to the W3C verifiable credentials model

The FIDO Authz Architecture



Web Site

FIDO Server

AA

User DB

Public Key DB

TLS

UAAF Protocol

TLS

UAAF Protocol

User's Browser

Web Site

Service Provider

FIDO Authz Module

FIDO Client

FIDO Server

Public Key/ Attribute DB

Authenticator Specific Module API

Public Key DB

Trusted Authenticators, AAs + Attestation Certs (out of band)

FIDO Authenticator

SOP Authn Keys

Certify Compliance

FIDO Metadata Service

Attestation Key

FIDO Ready Smart Device

Universal Authentication and Authorisation Framework (UAAF) Protocol

1. User registers her smart device at her Attribute Authorities (AAs) and consents to attributes being released as VCs
2. User accesses a Site (SP), starts a transaction, and SP sends its authorisation policy (in DNF or CNF) to the device
3. Device checks user has/can get VCs conforming to policy, and user chooses which VCs to use
4. Device requests VCs from her AAs
5. Device stores VCs for subsequent use
6. Device sends VCs to SP
7. SP asks user to confirm the transaction

User Registration at an AA

- User authenticates to AA with standard FIDO
- AA gets a new public key Pu_{AA} to associate with the user
- AA send set of assertable attributes to user's device
  - *AA*→*User*: *Attribute*$_1$…..*Attribute*$_n$
- User chooses which attributes can be released by AA (consent)
  - *User*→*AA*: *Attribute*$_i$…..*Attribute*$_j$
- Device's Authz Module records these

User Accesses Web Site

- User authenticates to web site with standard FIDO
- Web site gets new public key from user, Pu_{SP}
- User selects transaction
- Web site sends its Authorisation Policy to user's device
  - *SP→User*: *AuthzPolicy*
- Authz Module checks policy against attributes that can be asserted by trusted AAs
- Assuming user has sufficient AAs/attributes, transaction can progress

User Requests VCs

- For each AA that needs to issue VCs to the user

- User authenticates to AA and requests VCs

    - *User→AA*: {*Attribute*$_1$, *…, Attribute*$_n$, *nonce1, timestamp} SignPr*$_{AA}$

- AA responds with an encrypted nonce to user

    - *AA→User*: {*nonce*1, *nonce*2}*encrypted Pu*$_{AA}$

- Authorization module asks the authenticator to decrypt this, and then to sign two public keys, the AA's and the SP's, with the attestation private key to prove that both keys belong to the user, then returns proof of key ownership to AA

    - *User→AA*: {{*Pu*$_{SP}$, *Pu*$_{AA}$}*signed Pr*$_{Att}$,*nonce*2, *timestamp*}*signed Pr*$_{AA}$

- AA responds with a set of VC*s* specifically for the SP

    - *AA→User*:   *set of credentials* {*Pu*$_{SP}$, *Attribute*$_i$, *startTime*, *endTime*} *signed AA*

User Sends VCs to Web Site

- Authorisation Module collects sets of VCs from the AAs, stores them for subsequent use, then sends then to the web site, signed by private key specifically for this site to prove ownership
    - *User→Web Site*: {*credential*$_1$, …, *credential*$_n$, *nonce}signed Pr*$_{SP}$
- Web site now knows
    - some user, identified by the public key Pu$_{\mathrm{SP}}$, possesses the corresponding private key Pr$_{\mathrm{SP}}$,
    - this same user has a set of authorization attributes issued by a set of trusted AAs, because they all contain the same public key Pu$_{\mathrm{SP}}$,
    - all the attributes are still within their validity periods

Security and Privacy Benefits

- Not susceptible to phishing attacks
- Does not need user passwords for login
- Provides 2 factor Authn
- Provides Least Privileges by only releasing attributes that are needed for each transaction
- Provides Privacy Protection
  - User identified by site specific public key only

Privacy Issue

- Issuer (IdP) knows that a user has a set of key pairs, but does not know which public key is being sent to which Verifier (SP) or which SP the user is talking to
    - Nevertheless a rogue IdP could collude with a set of rogue SPs to check which public keys they have been sent
- HOWEVER, a rogue user cannot be blacklisted by an SP, because the user can return to the SP with a new key pair and VCs attached to the new public key
- Instead, the Verifier has to contact the Issuer, telling it that the user with this public key has committed this violation and rely on the Issuer to deal with it
- On balance we believe this potential privacy leakage is acceptable

Implementation

- Initial implementation performed by colleagues at Université Paul Sabatier, Toulouse
- Implemented in Java on a Google Nexus 5X running Android 6 (Marshmallow)
- Based on the FIDO UAF implementation of eBay
- Web sites built using the Spring framework
- Modified by University of Kent to support NHS use case and allow for transfer of VCs to a new smart device
- Toulouse has recently added an iPhone implementation

Transfer of VCs between devices

- User contacts her Issuers and asks them to create another set of VCs for a second device she owns
- Each Issuer sends an OTP to the original device, and these are passed to the second device using NFC or Bluetooth
- Second device creates a new key pair for each Issuer, then sends OTP to each one, which allows the Issuers to register the second device and public key for the user

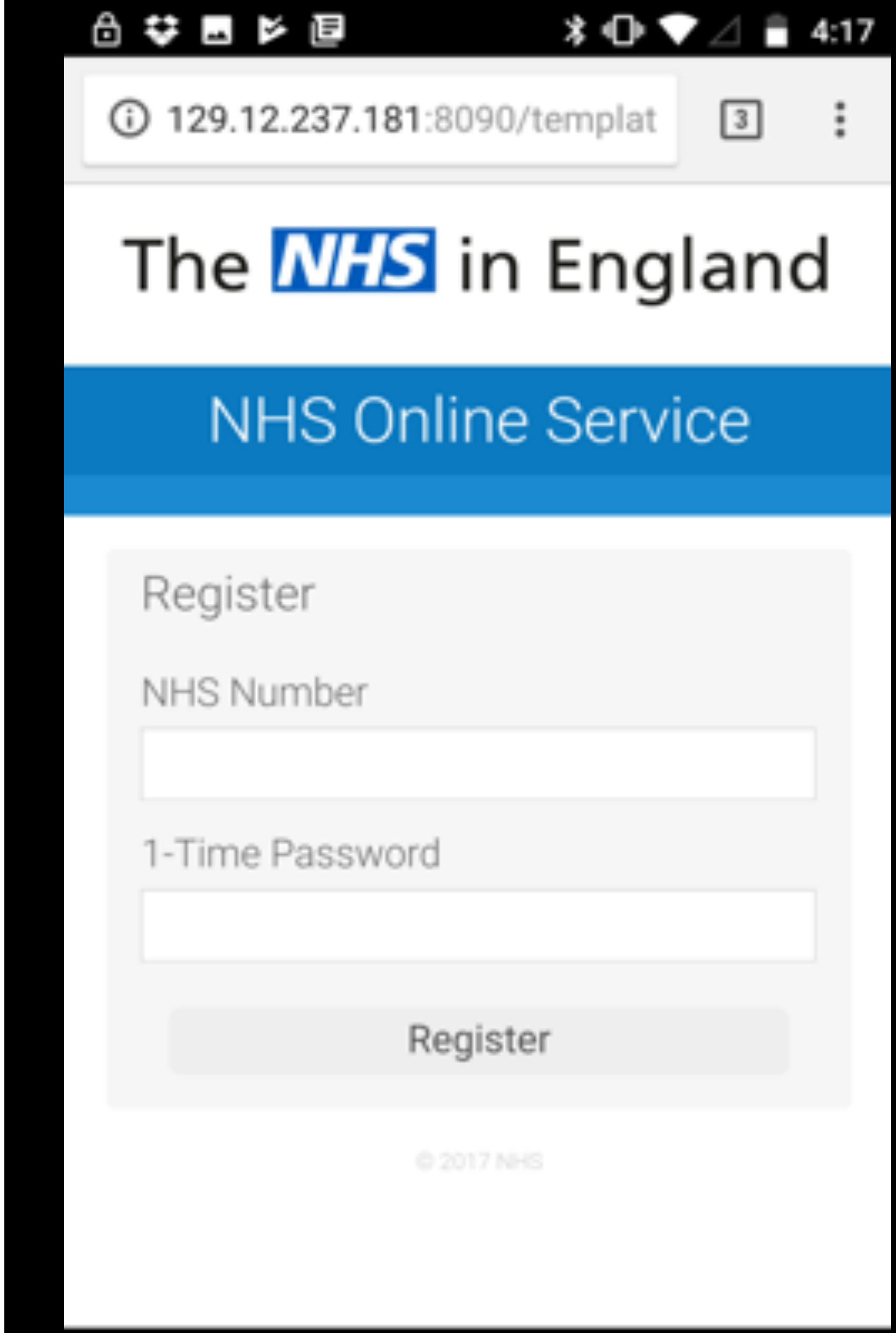
NHS Use Case

Missed GP and hospital appointments cost the English NHS nearly £1bn a year in 2015. Missed GP appointments alone cost £216M in 2018.

Repeat prescriptions can be time consuming requiring either two trips to the hospital or a long wait time

We developed an Android App to allow a patient to book and cancel a hospital appointment and to order repeat prescriptions

Registration Step 1. User registers with NHS Attribute Authority (using OTP posted to user's home address)



129.12.237.181:8090/templat

The NHS in England

NHS Online Service

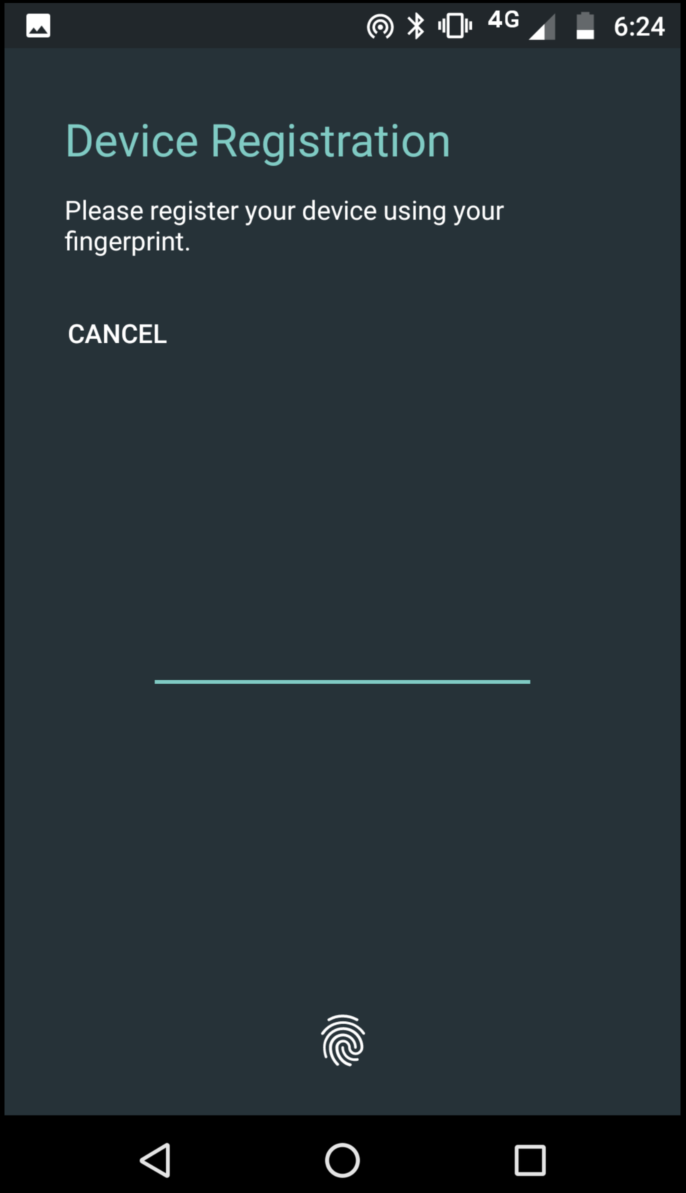
Register

NHS Number

1-Time Password

© 2017 NHS

Registration Step 2. User authenticates to phone by swiping finger, phone creates a new key pair and sends public key to the NHS AA

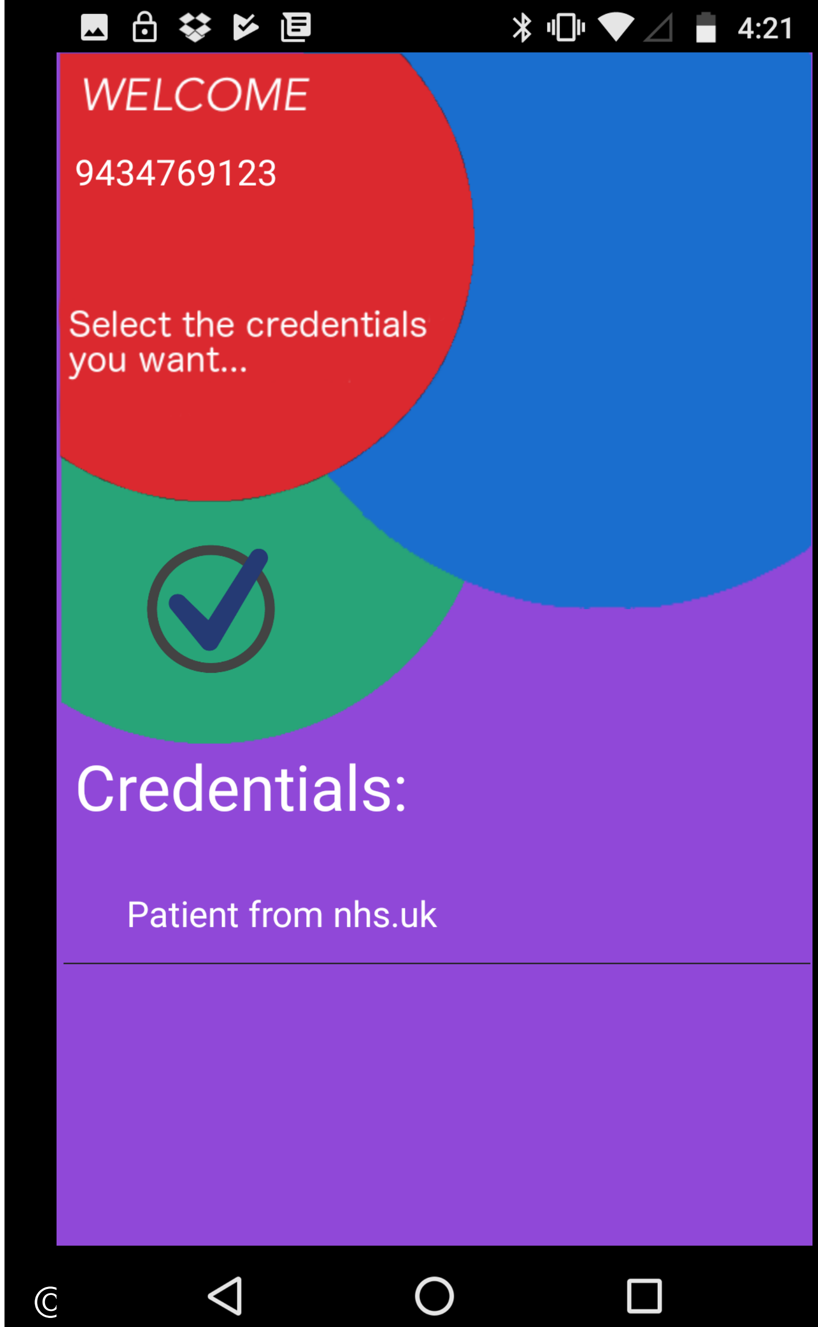


Device Registration

Please register your device using your fingerprint.

CANCEL

Registration Step 3. NHS asks user which credentials he wants. User chooses and NHS remembers (in this case there is no choice)



WELCOME

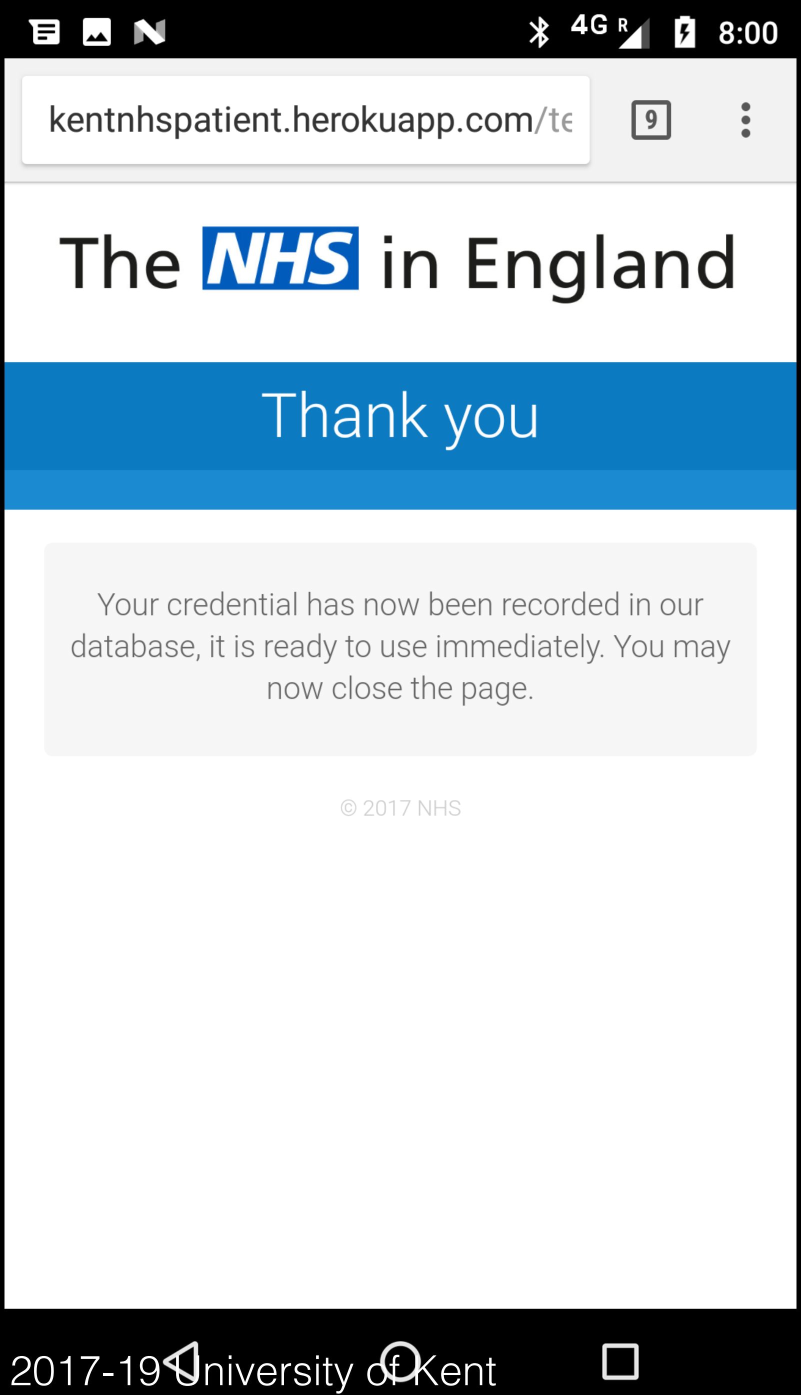
9434769123

Select the credentials you want...

Credentials:

Patient from nhs.uk

Registration Step 4. NHS confirms recording of credential



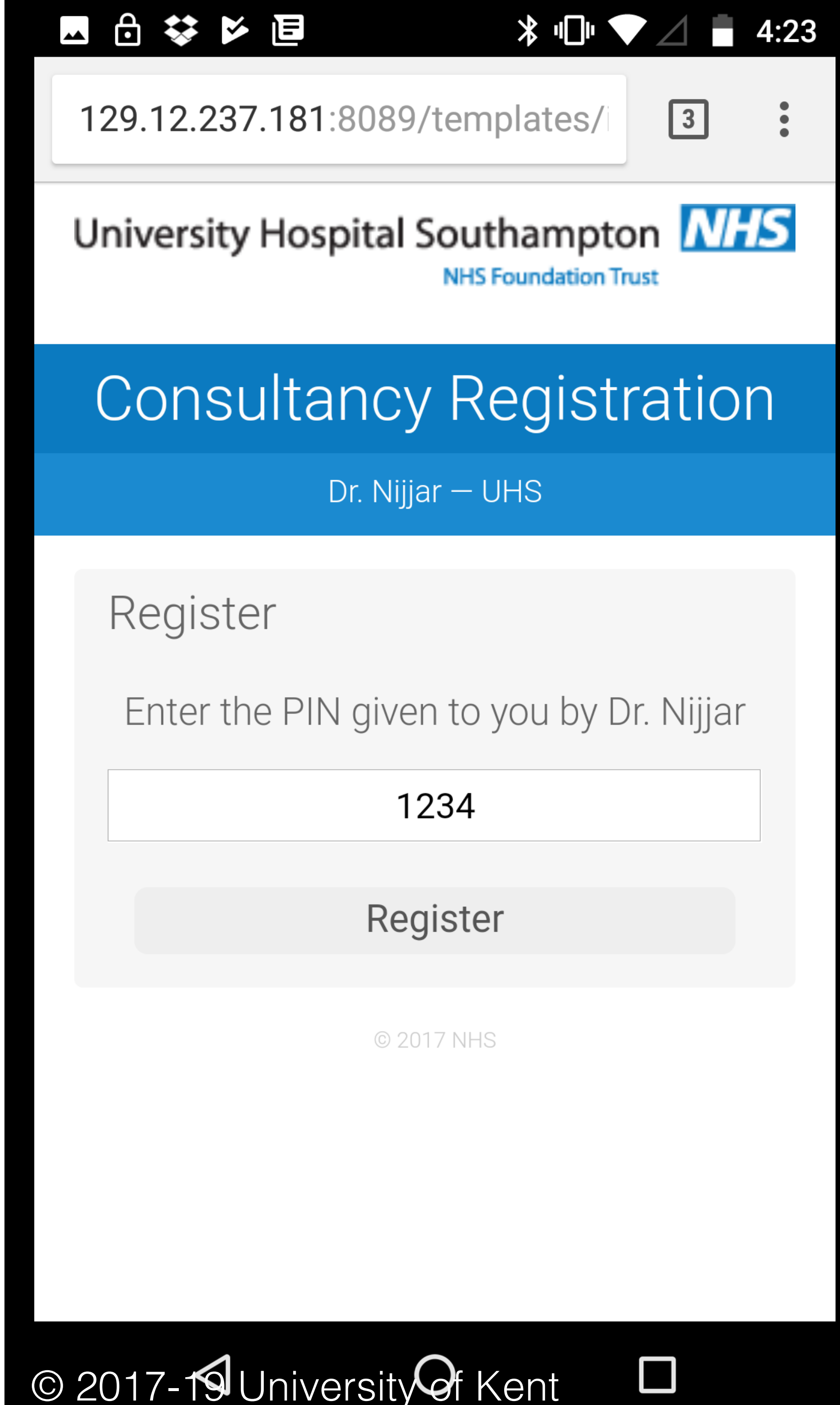
The NHS in England

Thank you

Your credential has now been recorded in our database, it is ready to use immediately. You may now close the page.

© 2017 NHS

Registration Step 5. The user goes to the hospital consultant and registers to use the consultant's service



129.12.237.181:8089/templates/i

University Hospital Southampton NHS
NHS Foundation Trust

Consultancy Registration

Dr. Nijjar — UHS

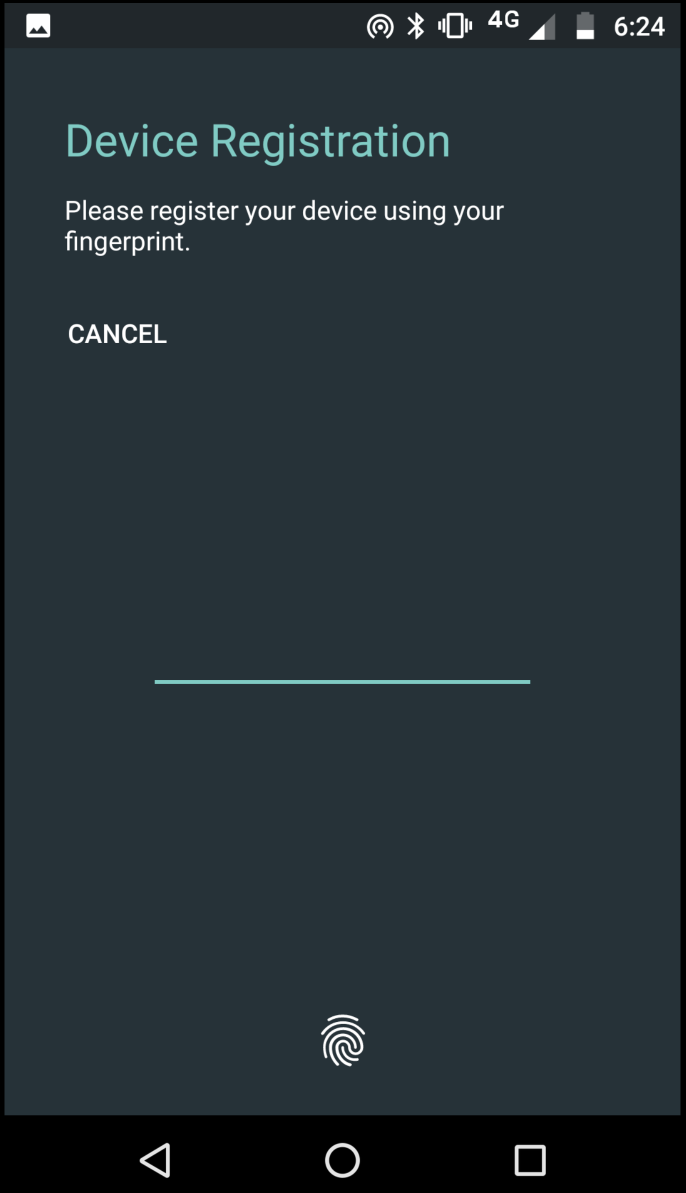
Register

Enter the PIN given to you by Dr. Nijjar

1234

© 2017 NHS

Registration Step 6. User authenticates to phone by swiping finger, phone creates a new key pair and sends public key to the Consultant’s AA

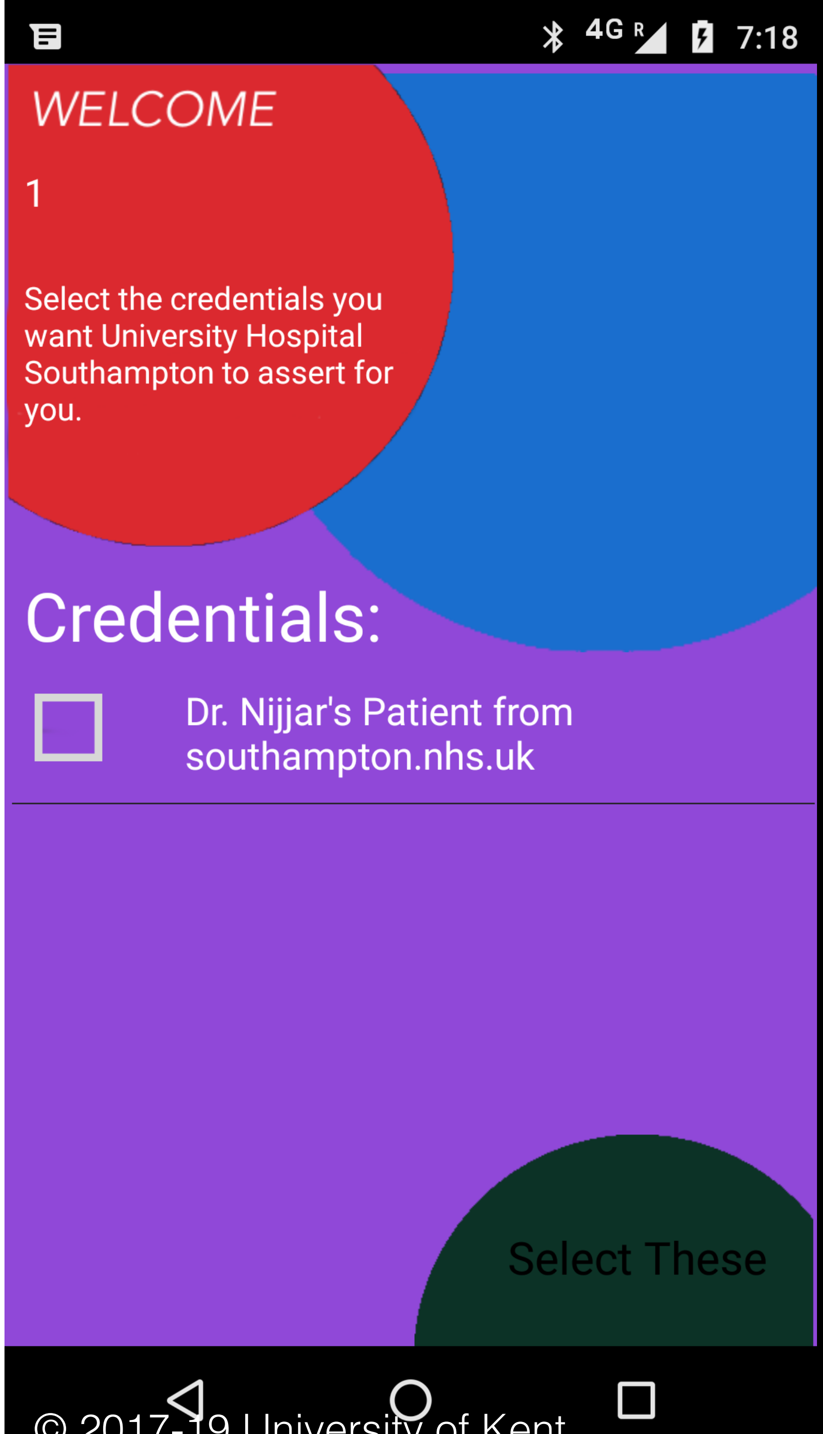


Device Registration

Please register your device using your fingerprint.

Registration Step 7. Consultant's AA asks user to select credentials to be asserted.

User chooses and AA remembers choice (in this case no choice)



WELCOME

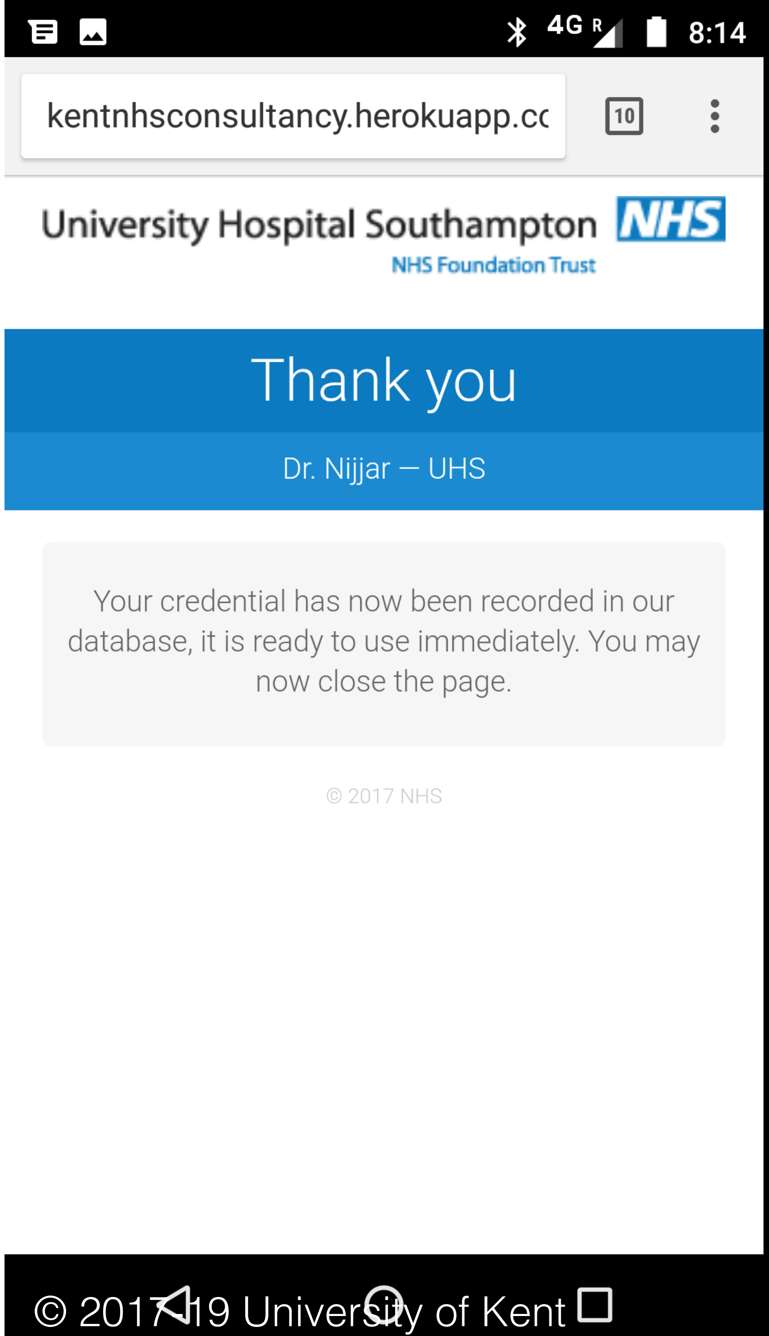
1

Select the credentials you want University Hospital Southampton to assert for you.

Credentials:

□ Dr. Nijjar's Patient from southampton.nhs.uk

Registration Step 8. Hospital confirms recording of credential


8:14
4G
kentnhsconsultancy.herokuapp.cc
10
University Hospital Southampton NHS
NHS Foundation Trust

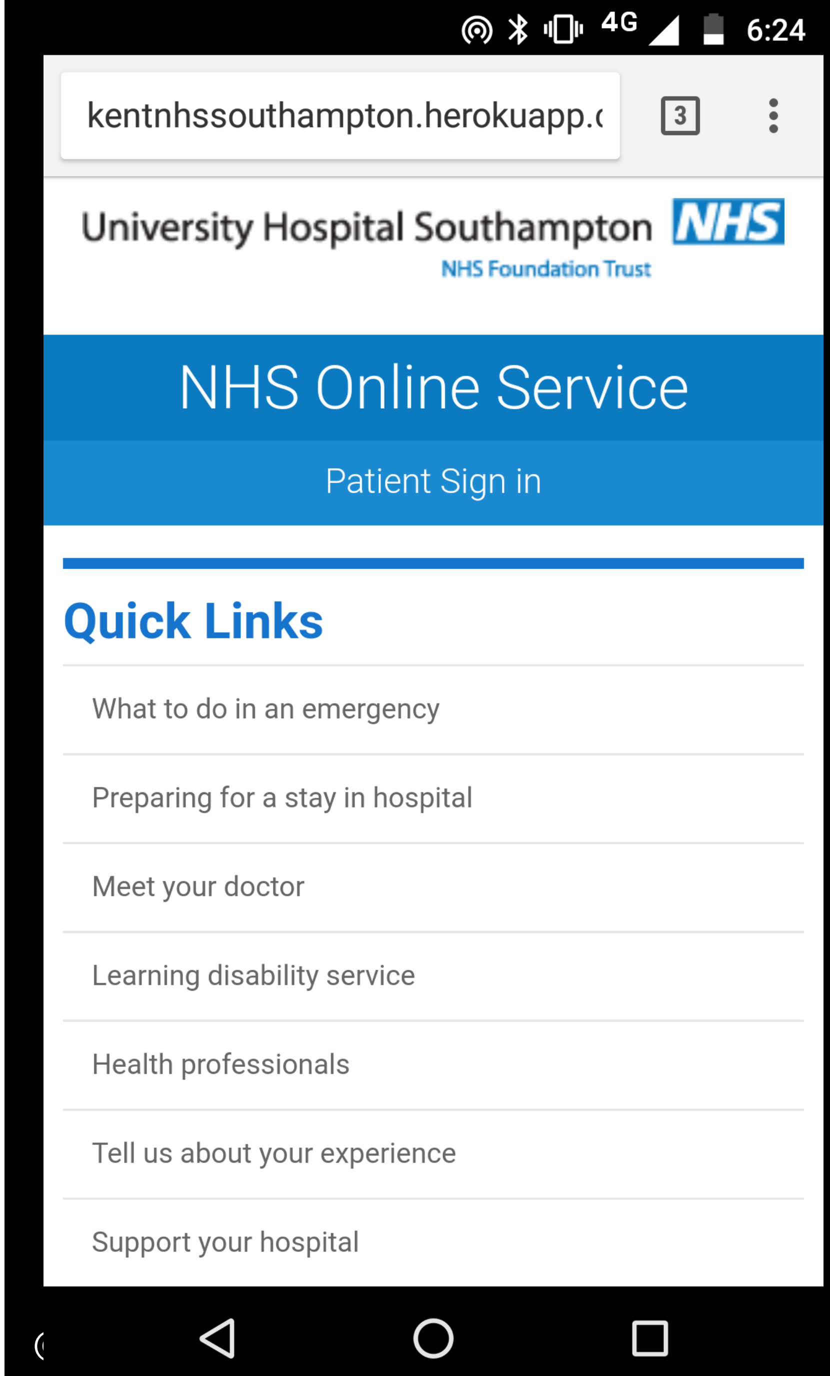
Thank you

Dr. Nijjar — UHS

Your credential has now been recorded in our database, it is ready to use immediately. You may now close the page.

© 2017 NHS

Use Step 1. User visits the hospital web site and signs in as an NHS patient



6:24

kentnhssouthampton.herokuapp.c

University Hospital Southampton NHS
NHS Foundation Trust

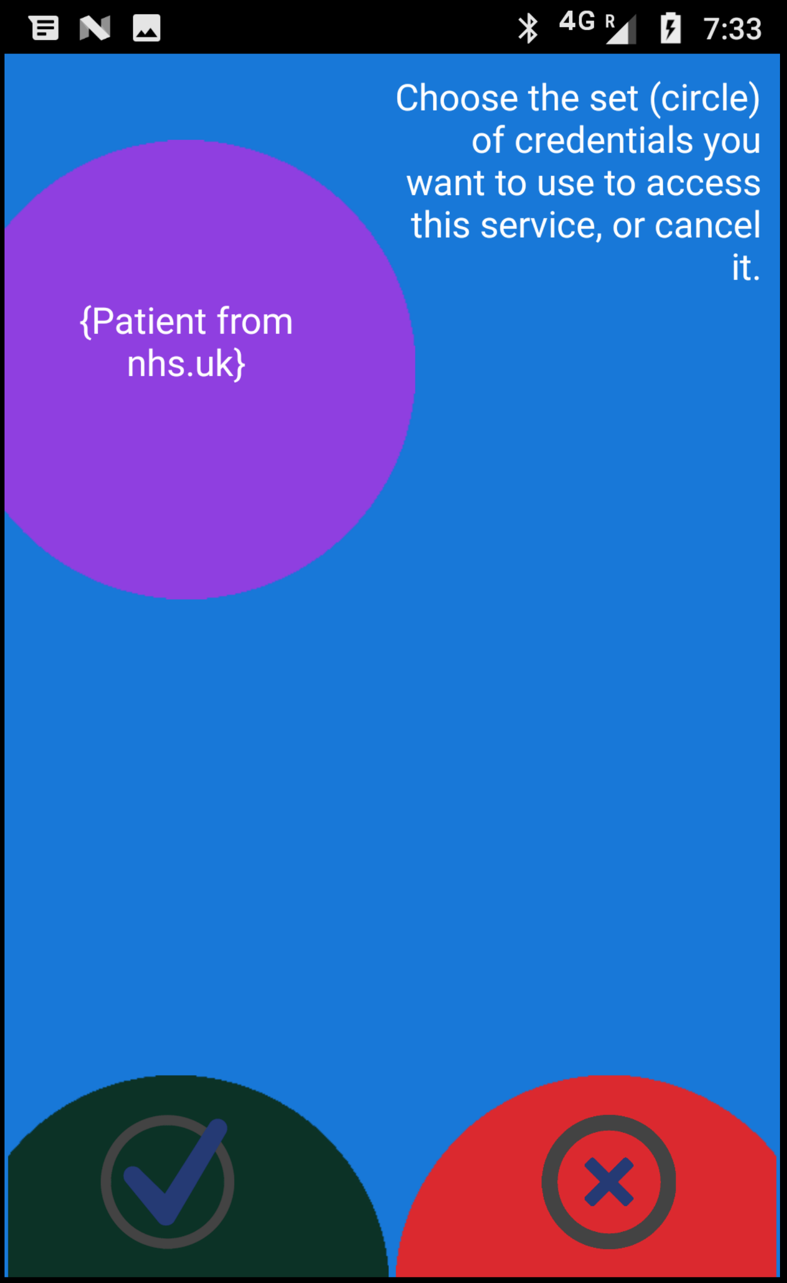
NHS Online Service

Patient Sign in

Quick Links

- What to do in an emergency
- Preparing for a stay in hospital
- Meet your doctor
- Learning disability service
- Health professionals
- Tell us about your experience
- Support your hospital

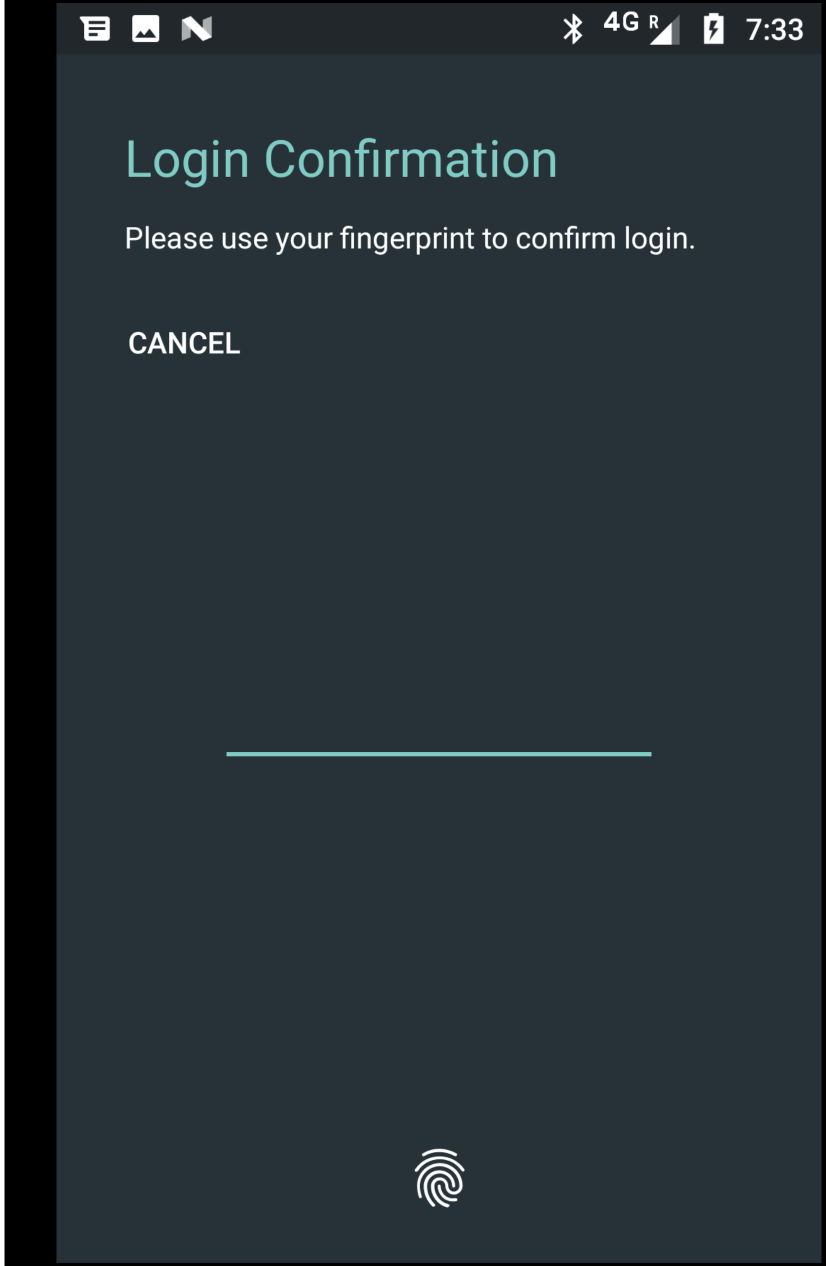
Use Step 2. Hospital sends its authz policy to the phone. Device matches policy against user's VCs and asks user to choose (no choice in this case)



Choose the set (circle) of credentials you want to use to access this service, or cancel it.

{Patient from nhs.uk}

Use Step 3. User confirms selection with fingerprint

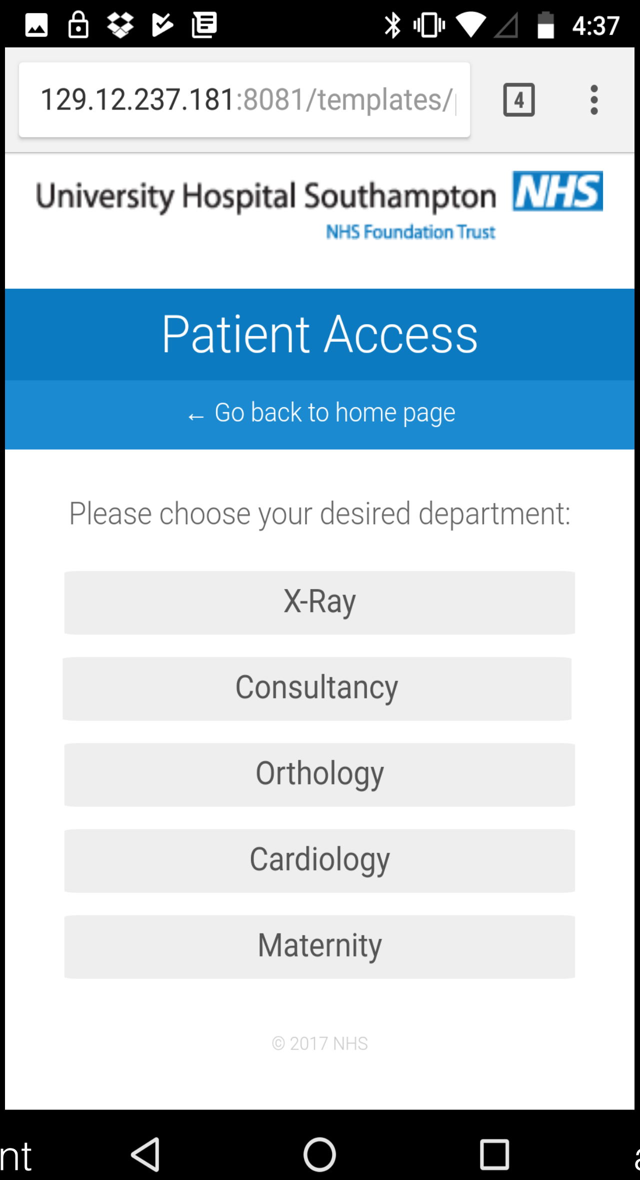


Login Confirmation

Please use your fingerprint to confirm login.

CANCEL

Use Step 4. Hospital Patient Menu is displayed. User chooses Consultancy



4:37

129.12.237.181:8081/templates/

University Hospital Southampton NHS
NHS Foundation Trust

Patient Access

← Go back to home page

Please choose your desired department:

X-Ray

Consultancy

Orthology

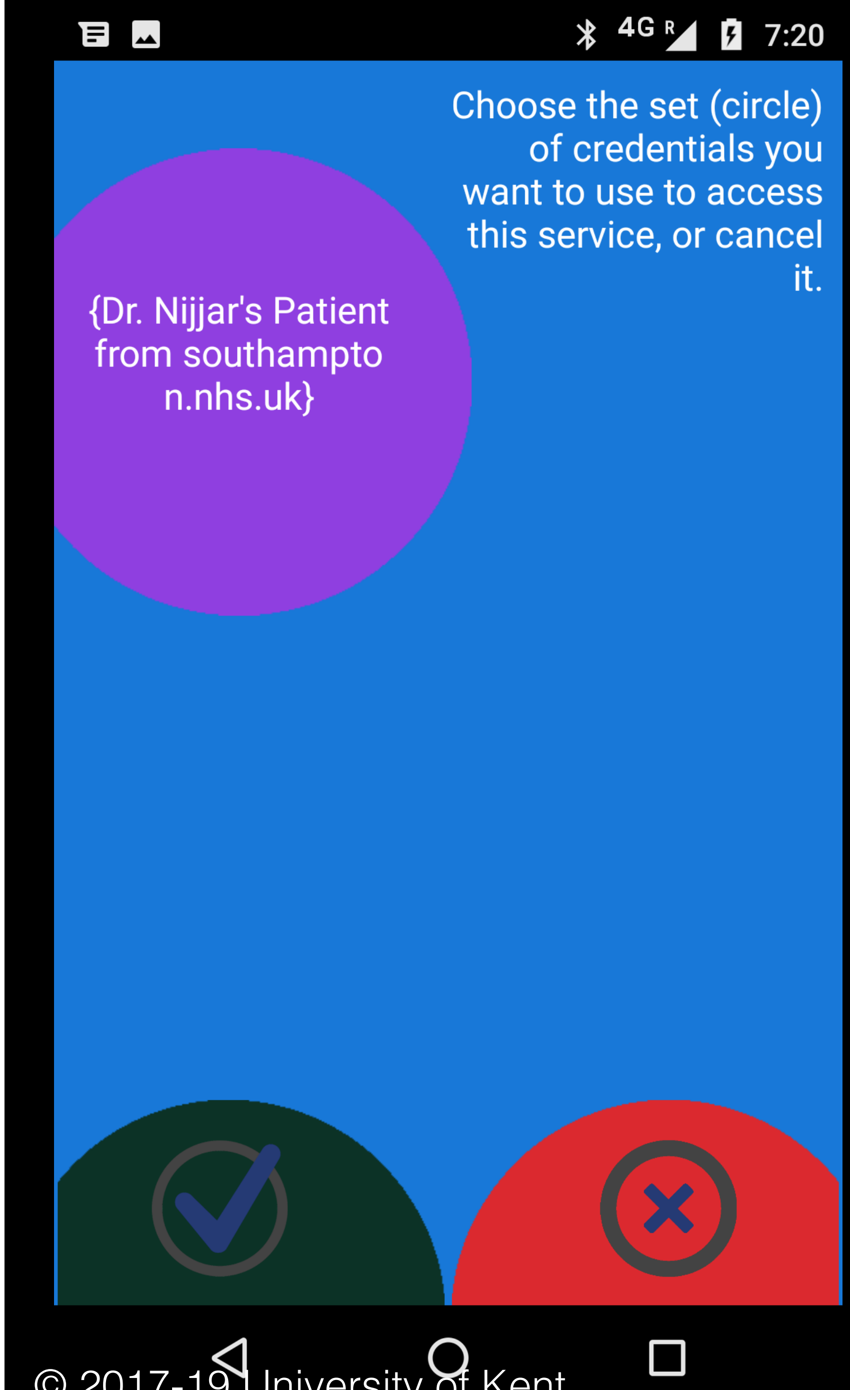
Cardiology

Maternity

© 2017 NHS

Use Step 5. Consultant's Authz policy is sent to phone.

Phone matches policy against VCs on phone and asks user to choose (no choice in this case)



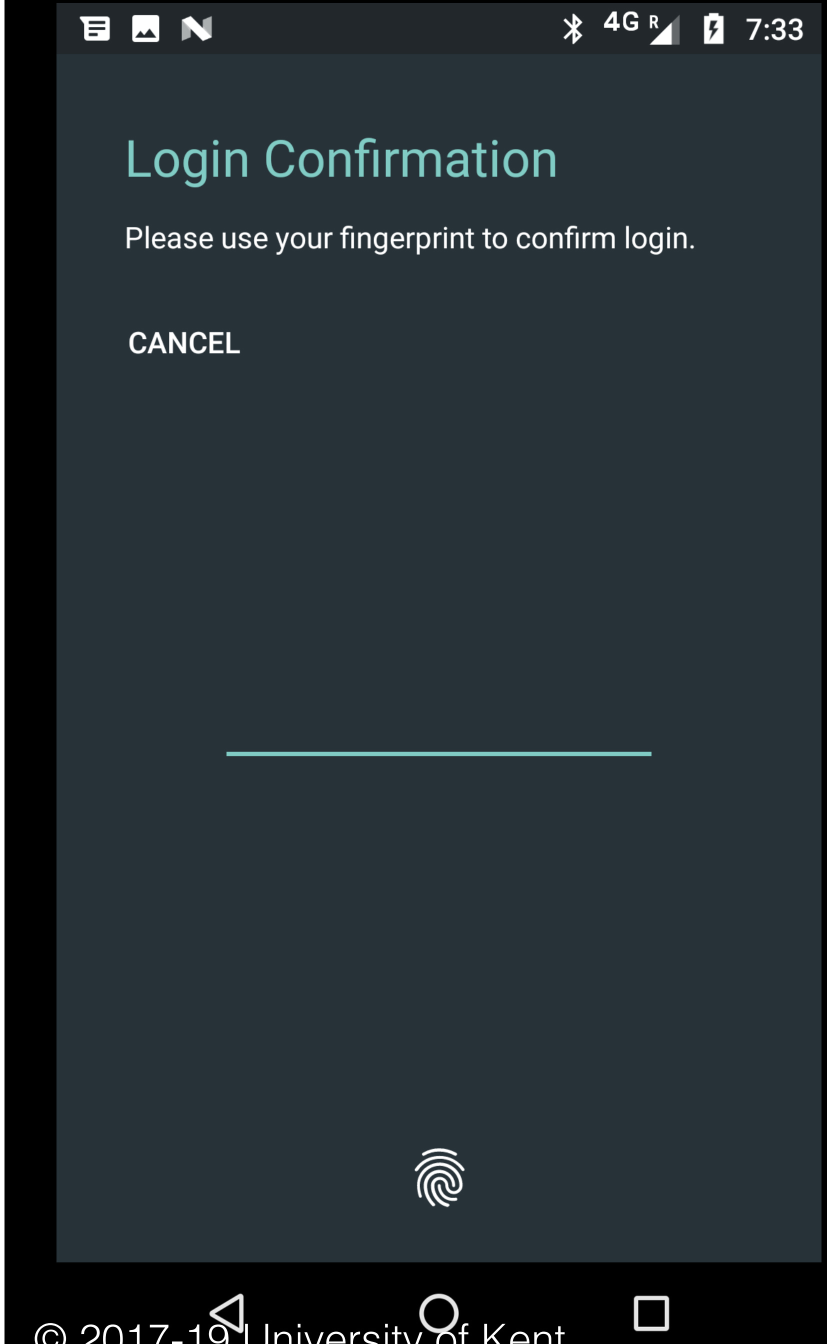
4G R 7:20

Choose the set (circle) of credentials you want to use to access this service, or cancel it.

{Dr. Nijjar's Patient from southampton.nhs.uk}

✓ ✗

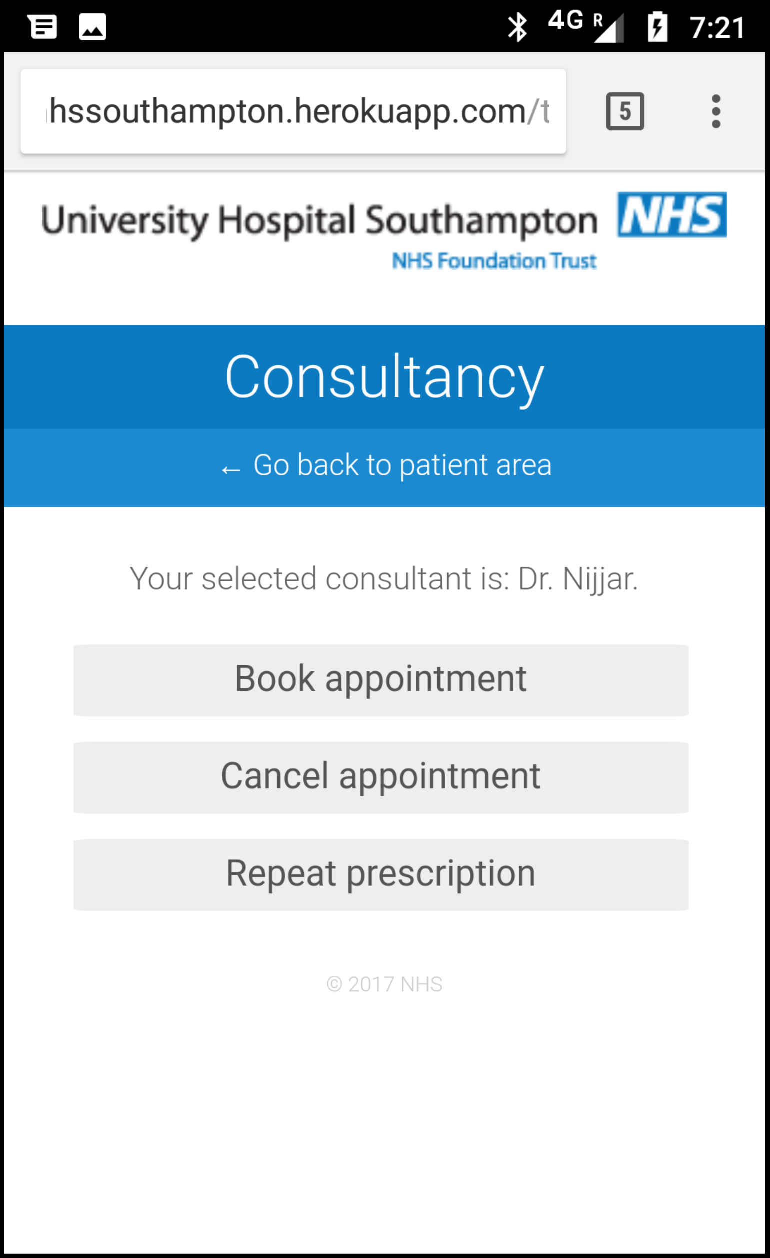
Use Step 6. User confirms selection with fingerprint



Login Confirmation

Please use your fingerprint to confirm login.

Use Step 7. Consultancy Menu is Displayed



4G R
7:21
hssouthampton.herokuapp.com/t
5
University Hospital Southampton NHS
NHS Foundation Trust

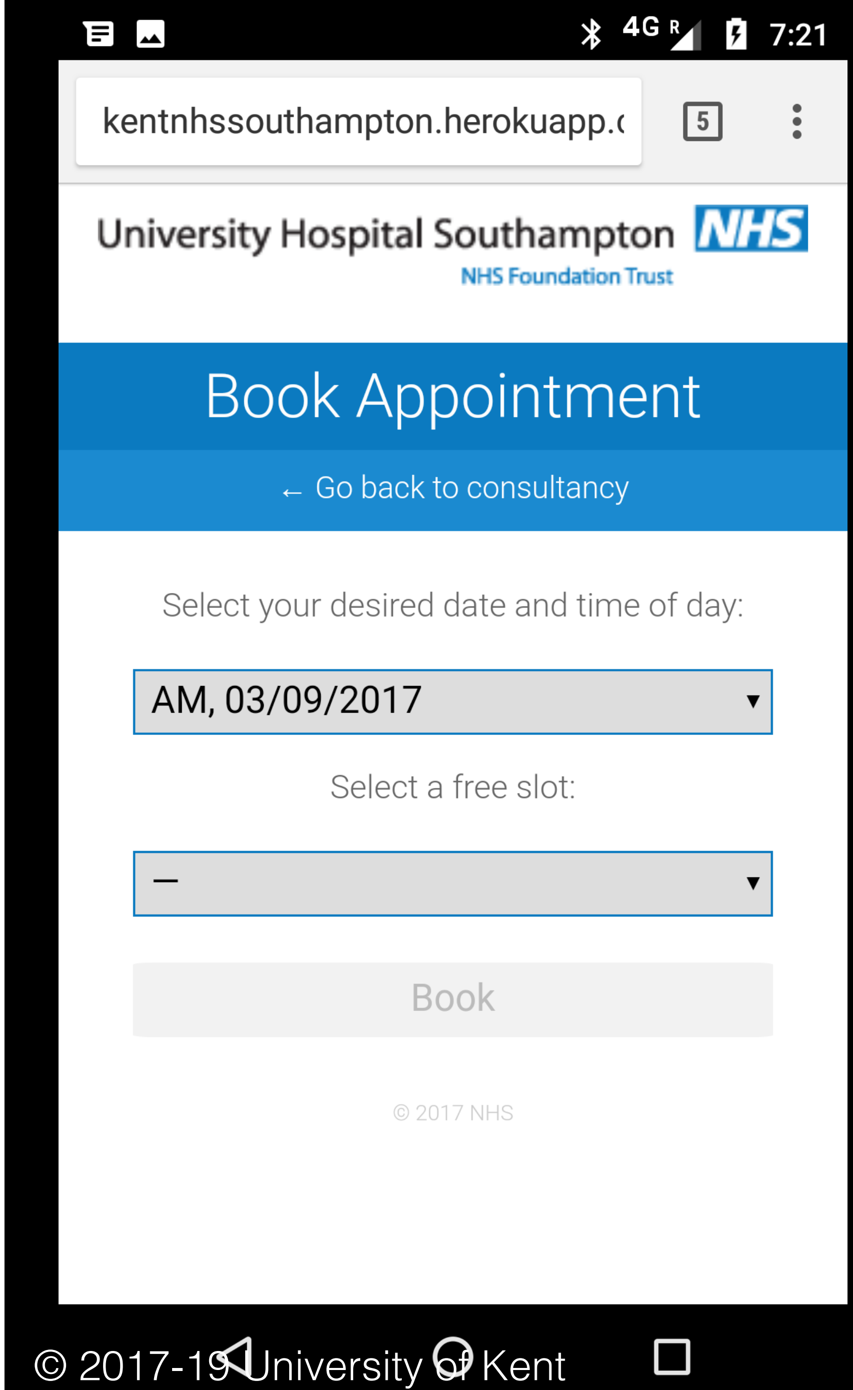
Consultancy

← Go back to patient area

Your selected consultant is: Dr. Nijjar.

© 2017 NHS

Use Step 9. Book Appointment



kentnhssouthampton.herokuapp.c

University Hospital Southampton NHS
NHS Foundation Trust

Book Appointment

← Go back to consultancy

Select your desired date and time of day:

AM, 03/09/2017 ▾

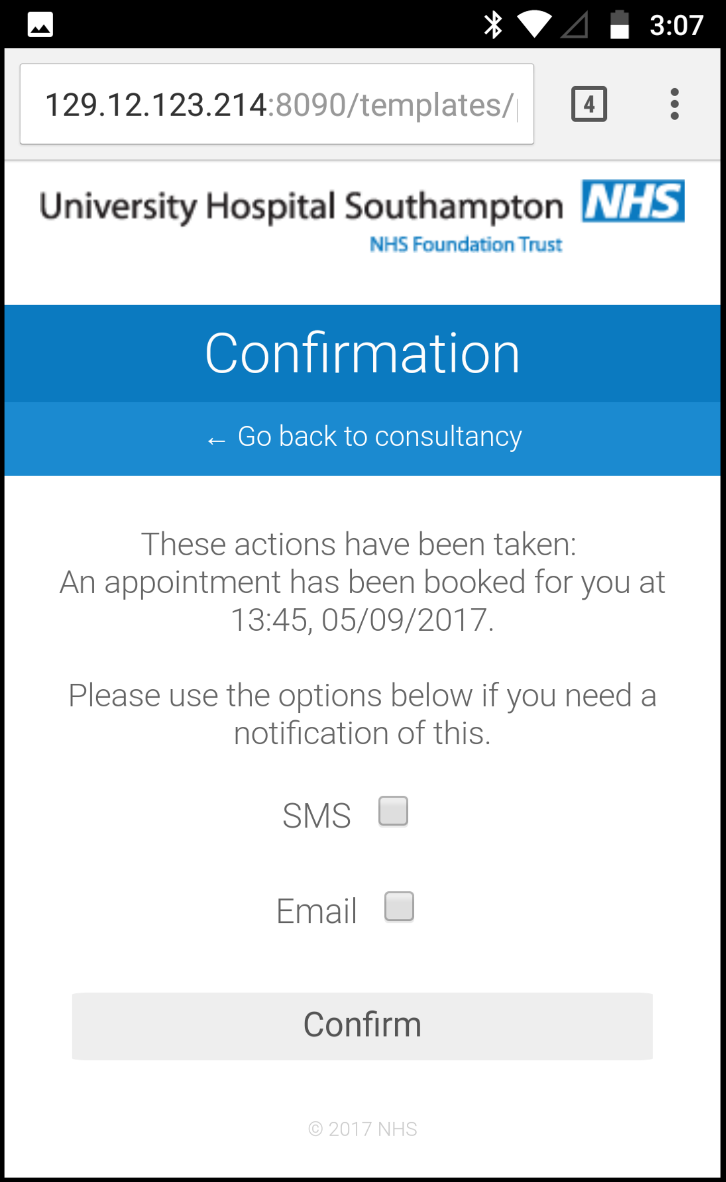
Select a free slot:

— ▾

Book

© 2017 NHS

Use Step 10. Confirmation Message



3:07
129.12.123.214:8090/templates/
4
University Hospital Southampton NHS
NHS Foundation Trust

Confirmation

← Go back to consultancy

These actions have been taken:
An appointment has been booked for you at 13:45, 05/09/2017.

Please use the options below if you need a notification of this.

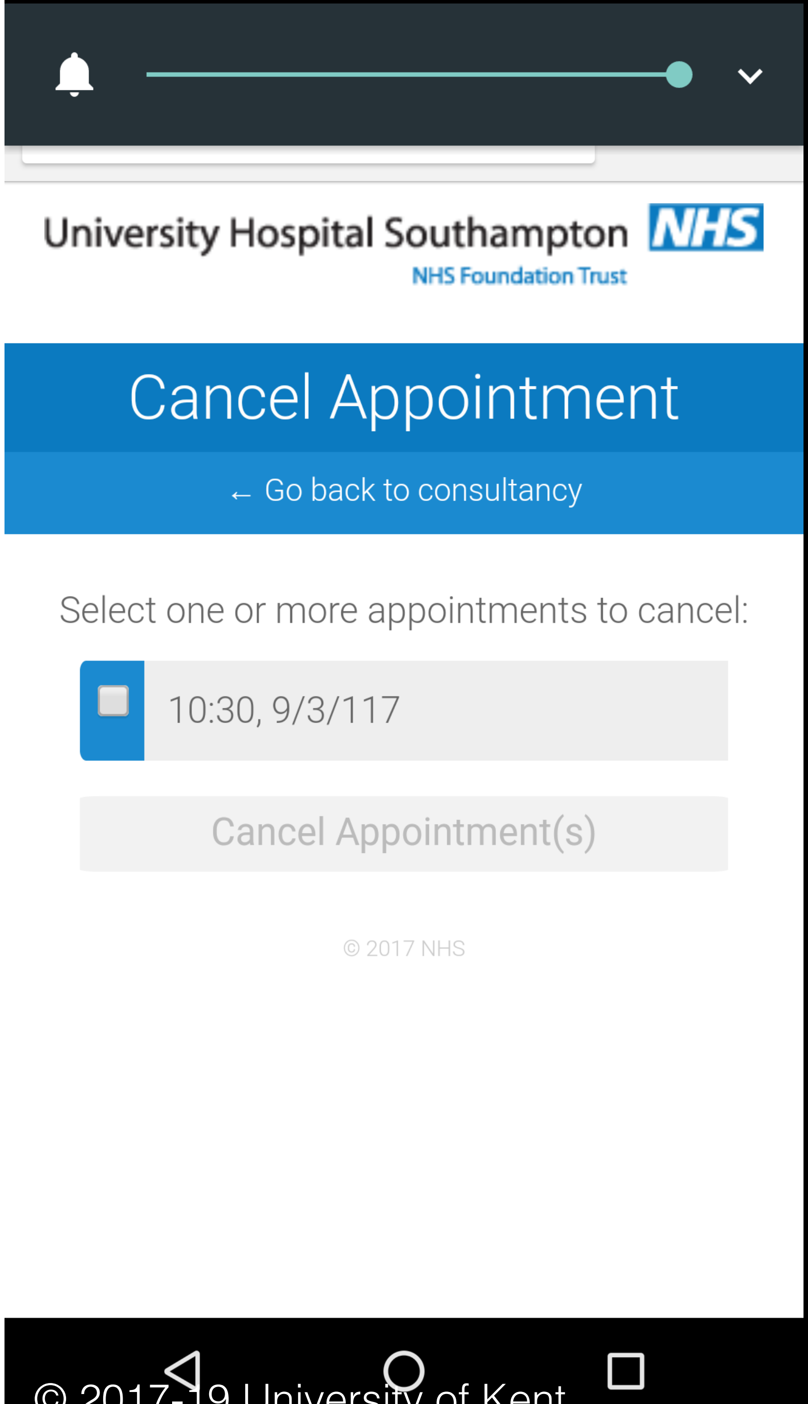
SMS □

Email □

Confirm

© 2017 NHS

Step 9. Cancel Appointment



University Hospital Southampton NHS
NHS Foundation Trust

Cancel Appointment

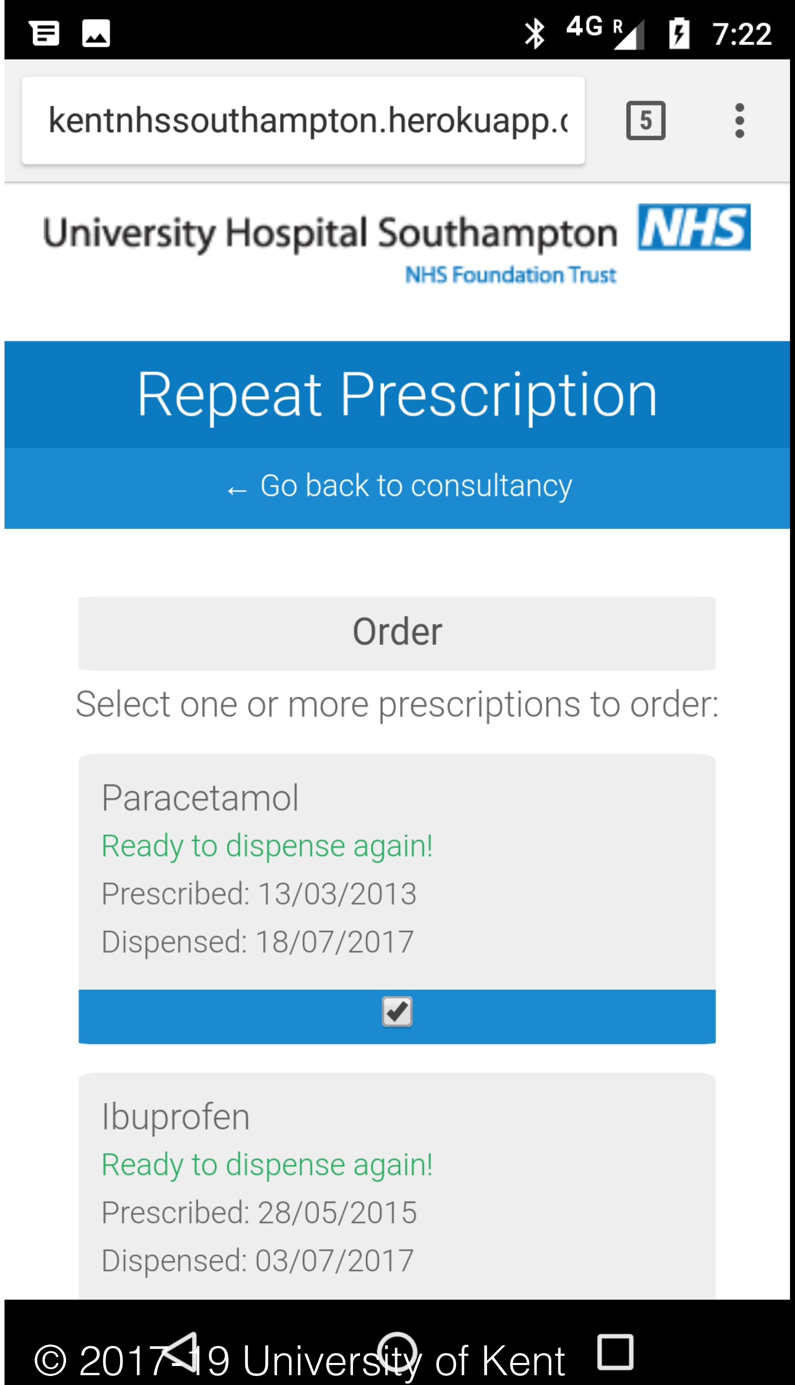
← Go back to consultancy

Select one or more appointments to cancel:

□ 10:30, 9/3/117

© 2017 NHS

Step 9. Order Repeat Prescription



4G R
7:22
kentnhssouthampton.herokuapp.c
5
University Hospital Southampton NHS
NHS Foundation Trust

Repeat Prescription

← Go back to consultancy

Order

Select one or more prescriptions to order:

Paracetamol
Ready to dispense again!
Prescribed: 13/03/2013
Dispensed: 18/07/2017

☑

Ibuprofen
Ready to dispense again!
Prescribed: 28/05/2015
Dispensed: 03/07/2017

Compliance with GDPR

- Makes SP compliance easier
- 6(1)(a) – Data subject has given consent
- 7(1) – Demonstrate consent
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject
- 5(1)(c) – Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- 5(1)(d) – Accurate and up to date
- 5(1) (f) – Processed in a manner that ensures appropriate security of the personal data
- 11 – Do not require the identification of a data subject

User Trials

- 10 hospital outpatients age <20 to >80
- Unanimously found the app easy to use and liked the use of fingerprints rather than usernames and passwords
- 1 user would prefer voice or iris scanning to fingerprints

Conclusion

- VCs are privacy protecting
  - Give the user full control of their identity
  - SP only obtains the attributes needed for authorisation and that the user consents to reveal
  - No globally unique correlating handle
  - IdP does not know which SP the user is visiting
- VCs protect against phishing attacks and identity theft
  - No SP login passwords, You would need to trick every Attribute Authority at registration time, and register before the real owner, in order to get their VCs, or
  - Steal the user’s phone and finger (or PIN) after he has registered
- VCs can be very easy to use and in our limited user trials were unanimously liked by patients

Any questions?