W3C Verifiable Credentials

David W Chadwick
University of Kent
Verifiable Credentials Ltd

Acknowledgements

This work was performed in collaboration with

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

And

Declan Barnes
University of Kent

And

Dr Manreet Nijjar
Truu ltd (previously Doctors Link Ltd)

The True Cost of Identity Theft

Will NEVER be known!!

But we have some estimates

- 173k people reported ID theft in the UK in 2016, total cost estimated at £5.4 billion
- 16.7M victims in US in 2017 at cost of $16 billion
- Over $107 billion in the U.S., in the past six years according to 2018 report by Javelin Strategy & Research

What are Verifiable Credentials?

- Potentially long-lived electronic credentials that users store under their control and use to identify themselves whenever they wish to access electronic resources

- Electronic equivalent of today's plastic cards, passports etc

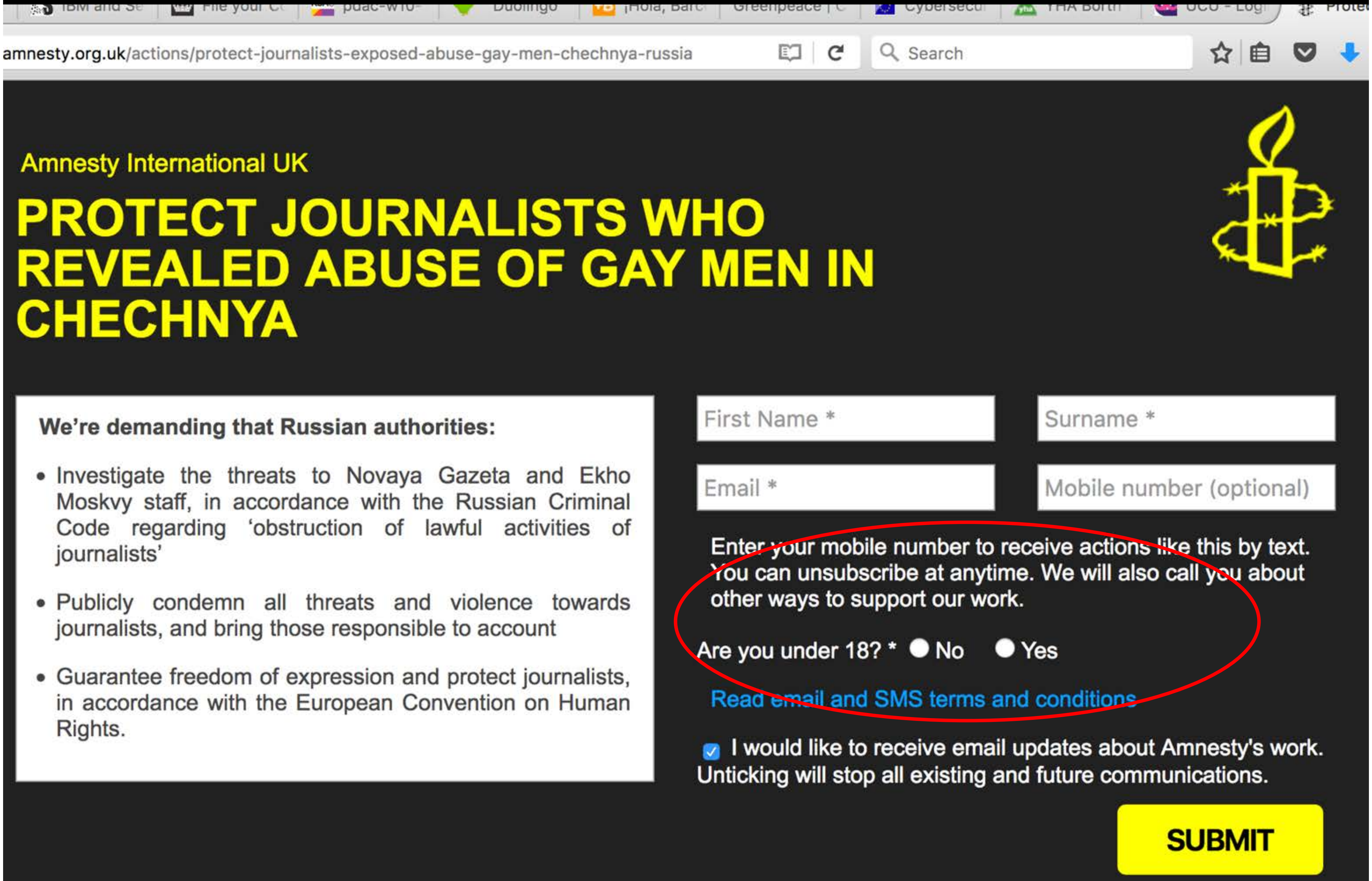
- Contain cryptographically protected identity attributes (PII)

- Used as Authorisation tokens in Attribute Based Access Control (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
- Because Identity Theft is a serious problem

Signing an Amnesty Petition – Are you under 18?



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.

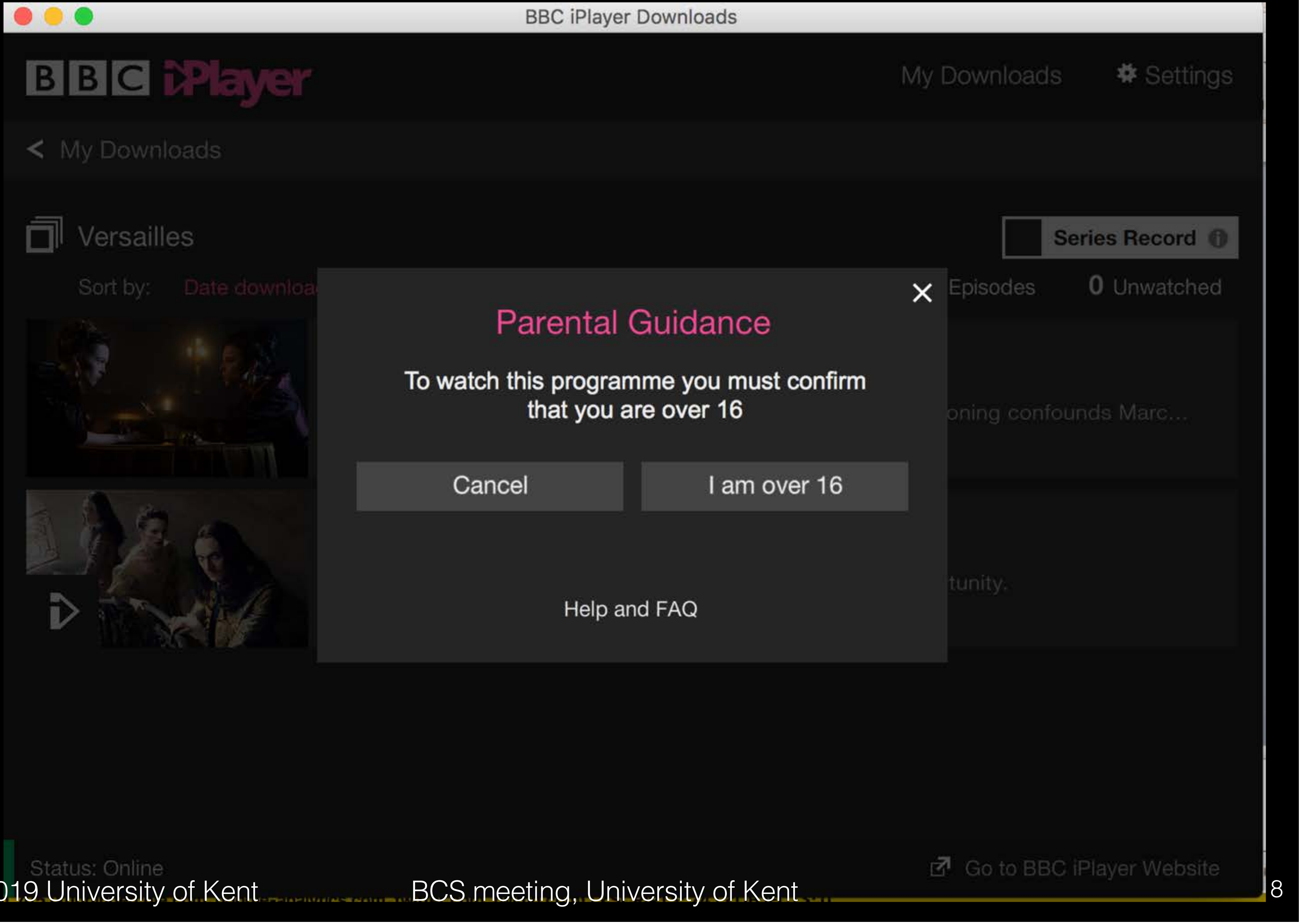
Are you under 18? * ○ No ○ Yes

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.

SUBMIT

BBC TV – Parental Guidance



Parental Guidance

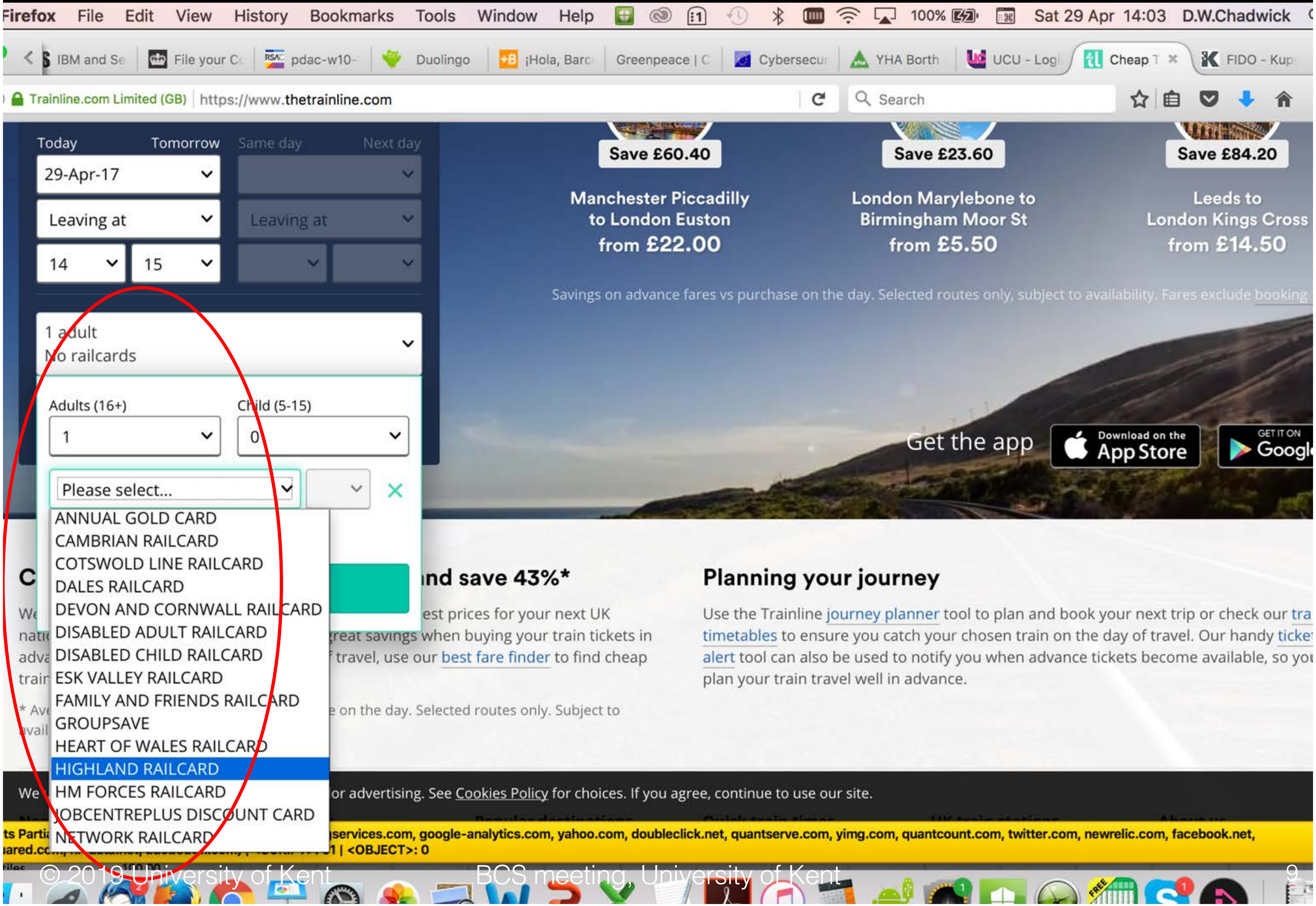
To watch this programme you must confirm that you are over 16

Cancel

I am over 16

Help and FAQ

Purchase a reduced price train ticket with a Railcard



Firefox File Edit View History Bookmarks Tools Window Help 100% Sat 29 Apr 14:03 D.W.Chadwick

IBM and Se | File your C | pdac-w10- | Duolingo | ¡Hola, Barc | Greenpeace | C | Cybersecu | YHA Borth | UCU - Logi | Cheap T | FIDO - Kup

Trainline.com Limited (GB) https://www.thetrainline.com Search

Today Tomorrow Same day Next day

29-Apr-17

Leaving at

14 15

Leaving at

1 adult
No railcards

Adults (16+) 1

Child (5-15) 0

Please select...

- ANNUAL GOLD CARD
- CAMBRIAN RAILCARD
- COTSWOLD LINE RAILCARD
- DALES RAILCARD
- DEVON AND CORNWALL RAILCARD
- DISABLED ADULT RAILCARD
- DISABLED CHILD RAILCARD
- ESK VALLEY RAILCARD
- FAMILY AND FRIENDS RAILCARD
- GROUPSAVE
- HEART OF WALES RAILCARD
- HIGHLAND RAILCARD
- HM FORCES RAILCARD
- JOBCENTREPLUS DISCOUNT CARD
- NETWORK RAILCARD

Save £60.40
Manchester Piccadilly to London Euston from £22.00

Save £23.60
London Marylebone to Birmingham Moor St from £5.50

Save £84.20
Leeds to London Kings Cross from £14.50

Savings on advance fares vs purchase on the day. Selected routes only, subject to availability. Fares exclude booking

C nd save 43%*

We est prices for your next UK nati reat savings when buying your train tickets in adva travel, use our best fare finder to find cheap trai

* Av e on the day. Selected routes only. Subject to avail

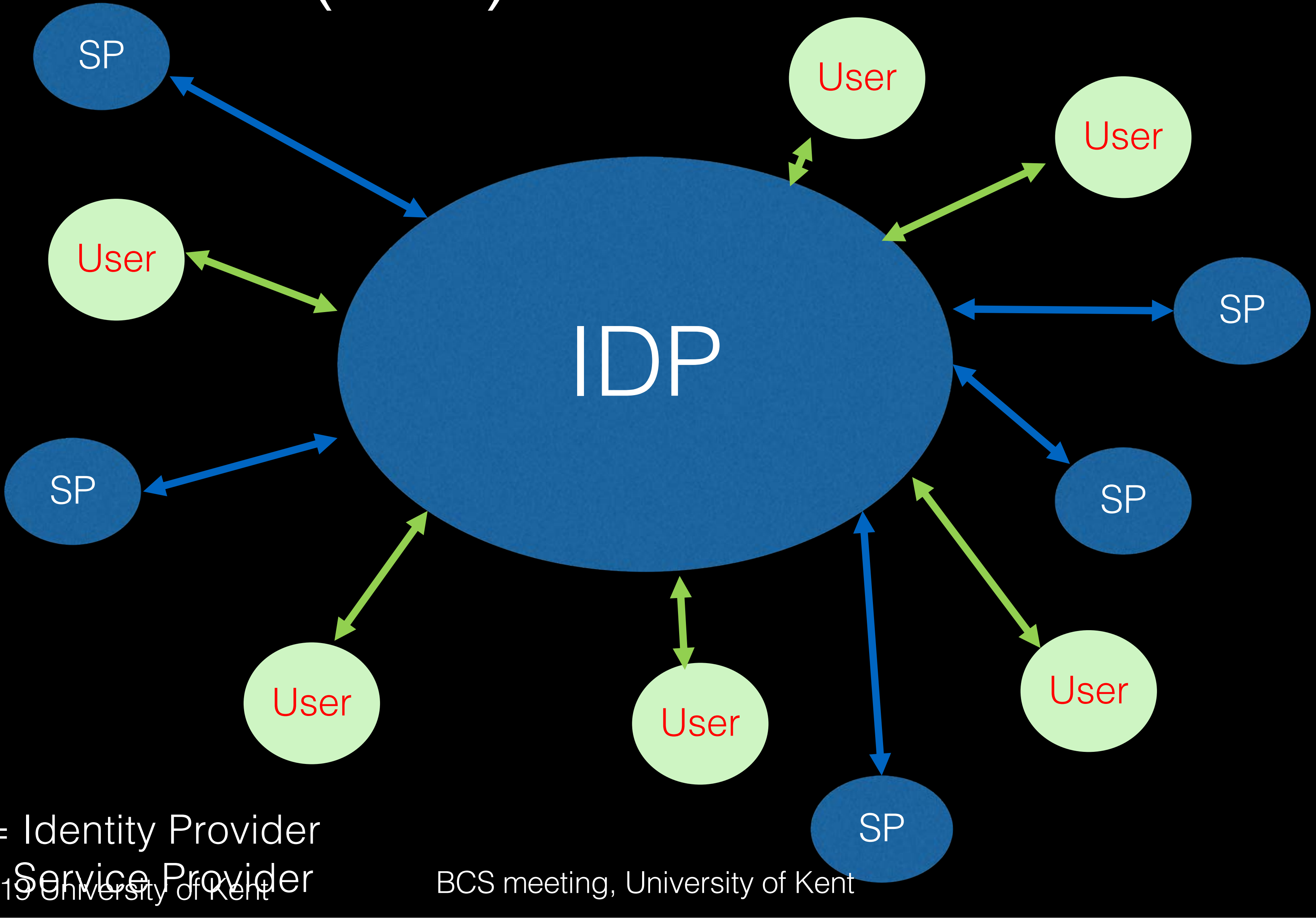
Planning your journey

Use the Trainline journey planner tool to plan and book your next trip or check our tra timetables to ensure you catch your chosen train on the day of travel. Our handy ticke alert tool can also be used to notify you when advance tickets become available, so you plan your train travel well in advance.

We or advertising. See Cookies Policy for choices. If you agree, continue to use our site.

ts Parti services.com, google-analytics.com, yahoo.com, doubleclick.net, quantserve.com, yimg.com, quantcount.com, twitter.com, newrelic.com, facebook.net, ared.co 1 | <OBJECT>: 0

Federated Identity Management (FIM) Limitations



IDP = Identity Provider

SP = Service Provider

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

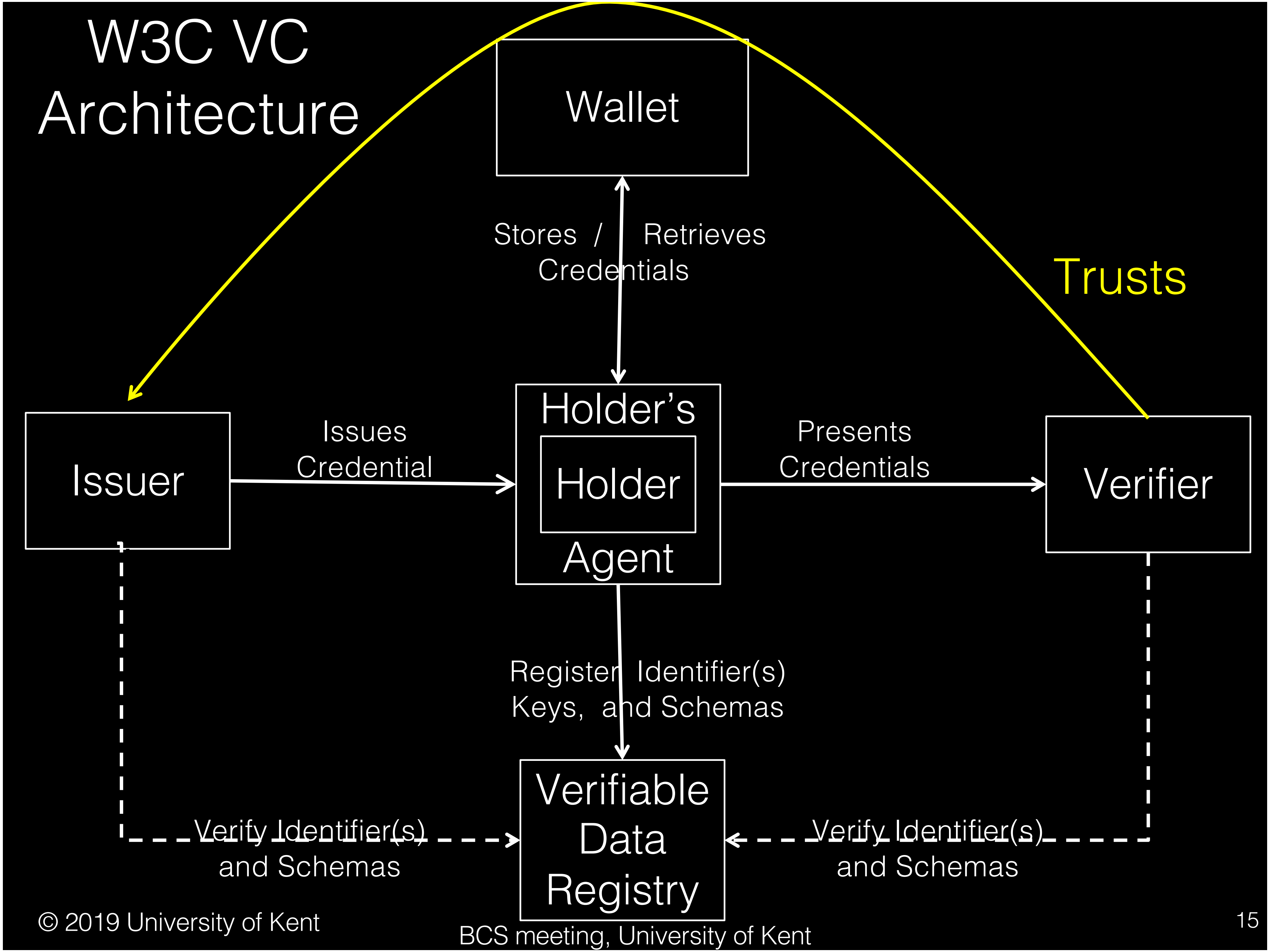
Compare FIM assertions to Plastic Cards, Passports etc.

- 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
Verify Identifier(s) and Schemas
Verifiable Data Registry
Verify Identifier(s) and Schemas

Verifiable Credentials Standardisation

- W3C VC Working Group only tasked with standardizing a data model for VCs
    - Specified in JSON-LD
    - Allows any type of crypto to protect it
- Has just finished work and Proposed Recommendation published in September 2019

A W3C Verifiable Credential

```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/3732",
    "type": ["VerifiableCredential", "UniversityDegreeCredential"],
    "issuer": "https://example.edu/issuers/14",
    "issuanceDate": "2010-01-01T19:23:24Z",
    "expirationDate": "2020-01-01T19:23:24Z",
    "credentialSubject": {
        "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
        "degree": {
            "type": "BachelorDegree",
            "name": "Bachelor of Science and Arts"
        }
    },
    "proof": { …}
}
```

@Context

- Used to map globally unique URIs into user friendly aliases

- To avoid the user-unfriendliness of OIDs as used in X.509 e.g. 2.5.4.3.1

- To avoid the local name clashes of LDAP / MS AD e.g. is my ‘telno’ the same as yours or her ‘telephone_number’

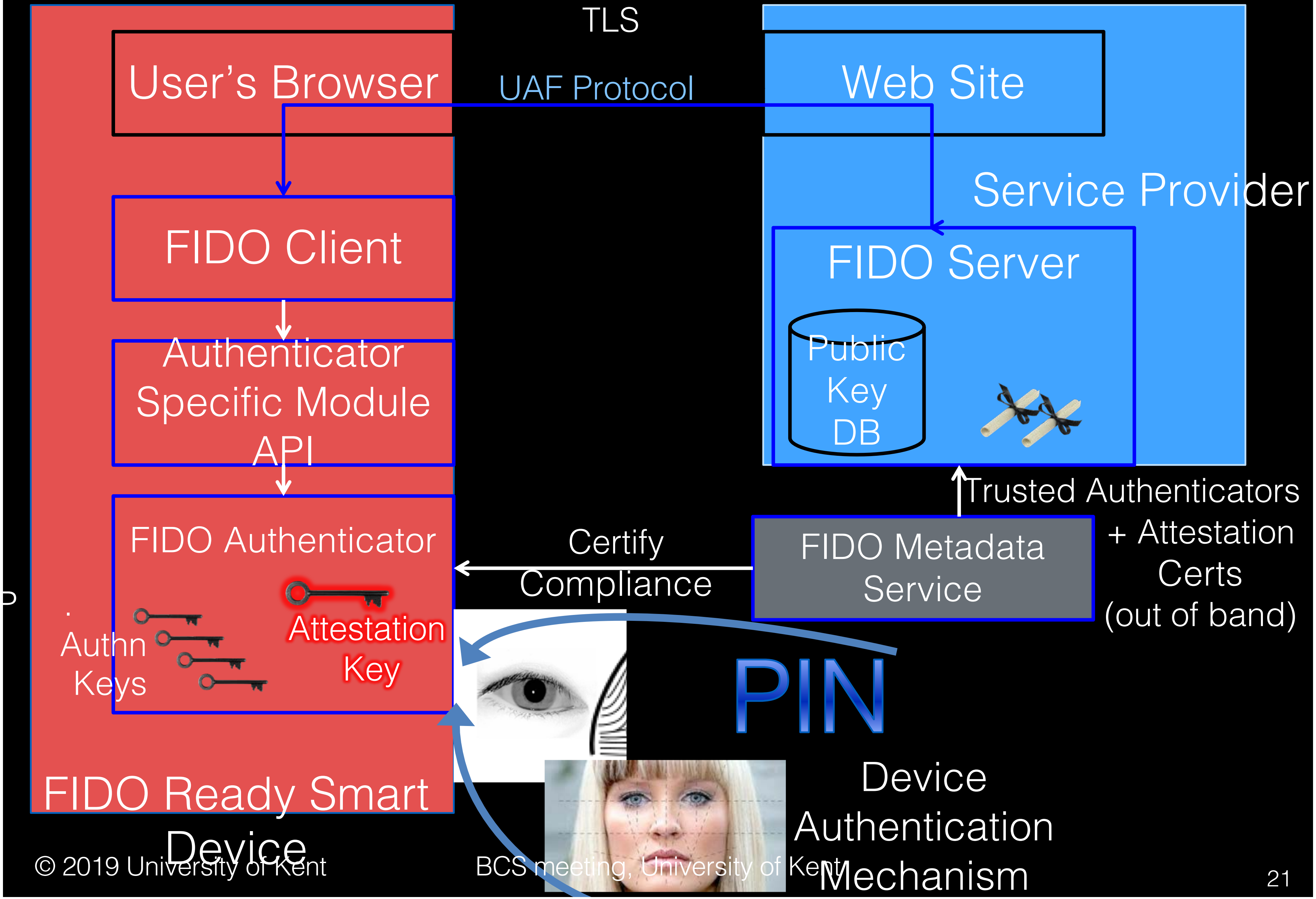
But…

- Protocols are out of scope of W3C VC WG
- W3C Credentials Community Group may now incubate them
- But until then we are on our own, SO>>>>>
    - We defined our own protocol based on FIDO

Fast Identity Online - FIDO

- The FIDO Alliance originally developed the original FIDO specifications for strong authentication in 2014
- Then took them to W3C for standardization, which published the Web Authentication Recommendation in 2019 (FIDO2)
- Uses asymmetric encryption, with a unique key pair created for every web site the user visits
- Two original FIDO specifications merged into WebAuthn
    - 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

Authenticator Specific Module API

Public Key DB

Trusted Authenticators + Attestation Certs (out of band)

FIDO Authenticator

Authn Keys

Attestation Key

Certify Compliance

FIDO Metadata Service

PIN

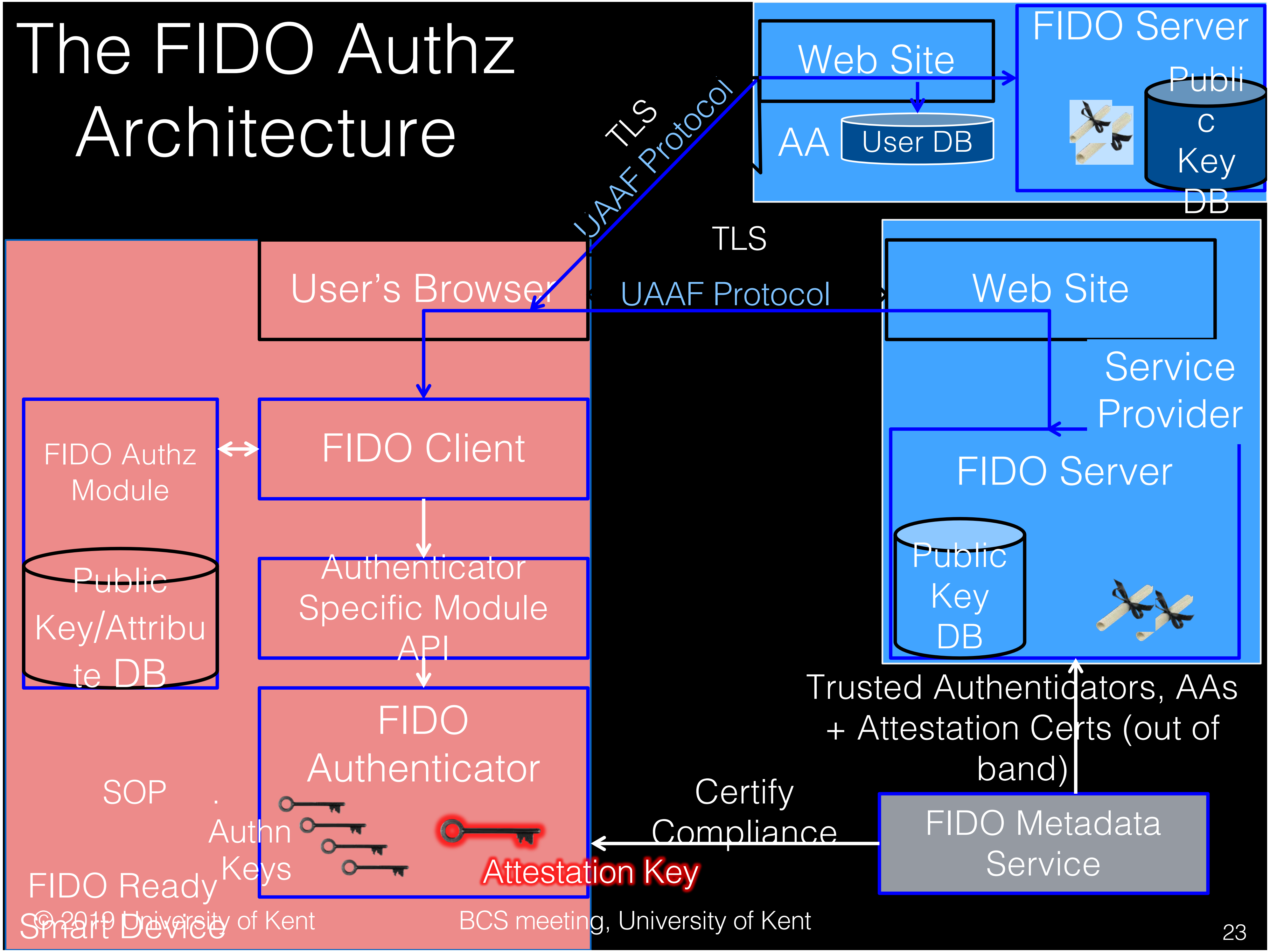
Device Authentication Mechanism

FIDO Ready Smart Device

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/FIDO2, that conforms to the W3C verifiable credentials model

The FIDO Authz Architecture



FIDO Server

Web Site

Publi c Key DB

AA

User DB

TLS

UAAF Protocol

TLS

UAAF Protocol

User's Browser

Web Site

Service Provider

FIDO Authz Module

FIDO Client

FIDO Server

Public Key/Attribu te DB

Authenticator Specific Module API

Public Key DB

FIDO Authenticator

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

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 FIDO keys at her IdPs and consents to her attributes being released as VCs

2. User accesses a Site (SP), asks to access a protected resource, and SP sends its identification policy (in DNF or CNF) to the device

3. Device checks if user has/can get VCs conforming to the ID 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 grants user access to resource

Security and Privacy Benefits

- Not susceptible to phishing attacks
- Protects against Identity Theft with cryptographic credentials
- Does not need user passwords for login
- Provides 2 factor Authn (FIDO key and Biometric/PIN to access it)
- Provides Least Privileges by only releasing attributes that are needed for each transaction
- Provides Privacy Protection and aids compliance with GDPR
    - User authenticated by site specific public key only

Compliance with GDPR

- Makes SP compliance easier
- 6(1)(a) – Data subject has given consent to both IdP and SP
- 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

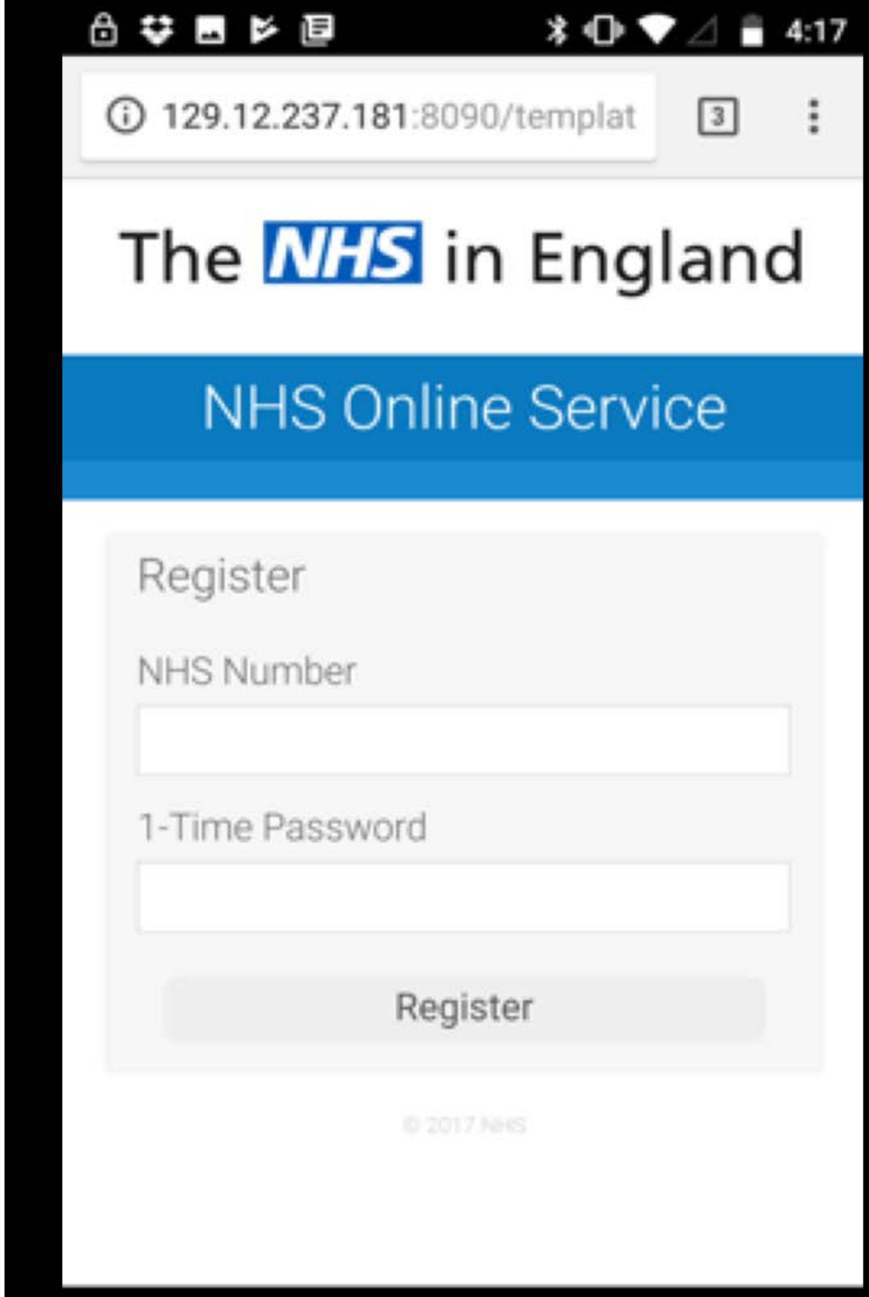
NHS Use Case

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

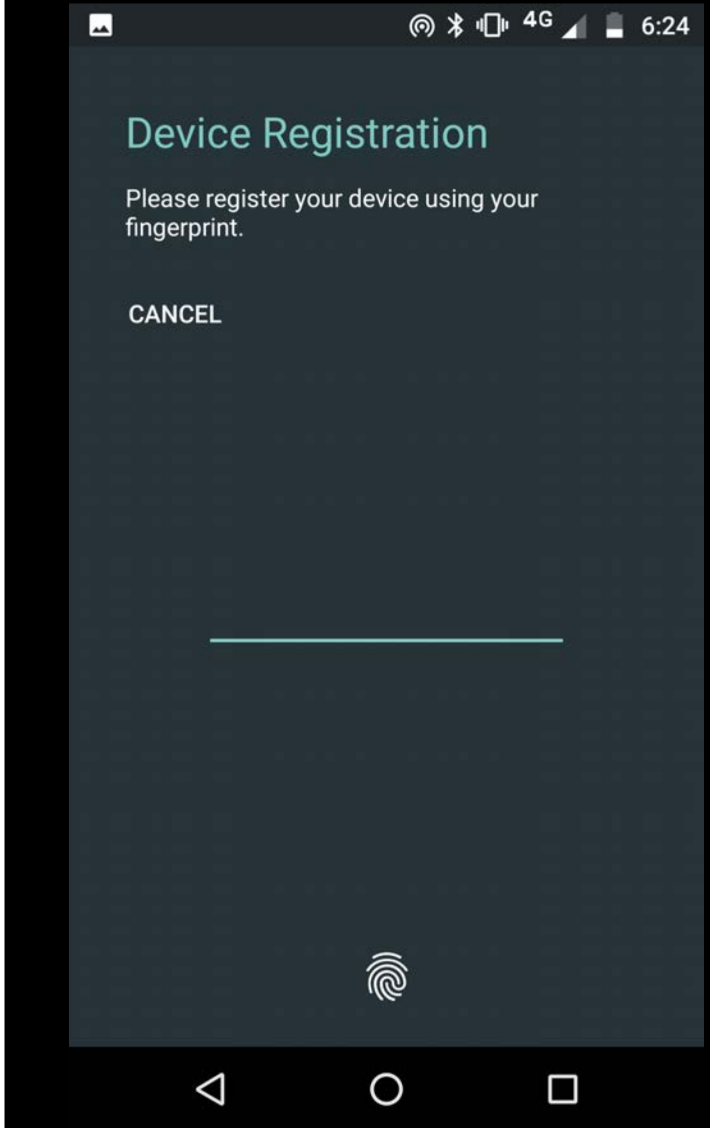
Repeat prescriptions can be time consuming requiring either two trips to the hospital or a long wait time

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)



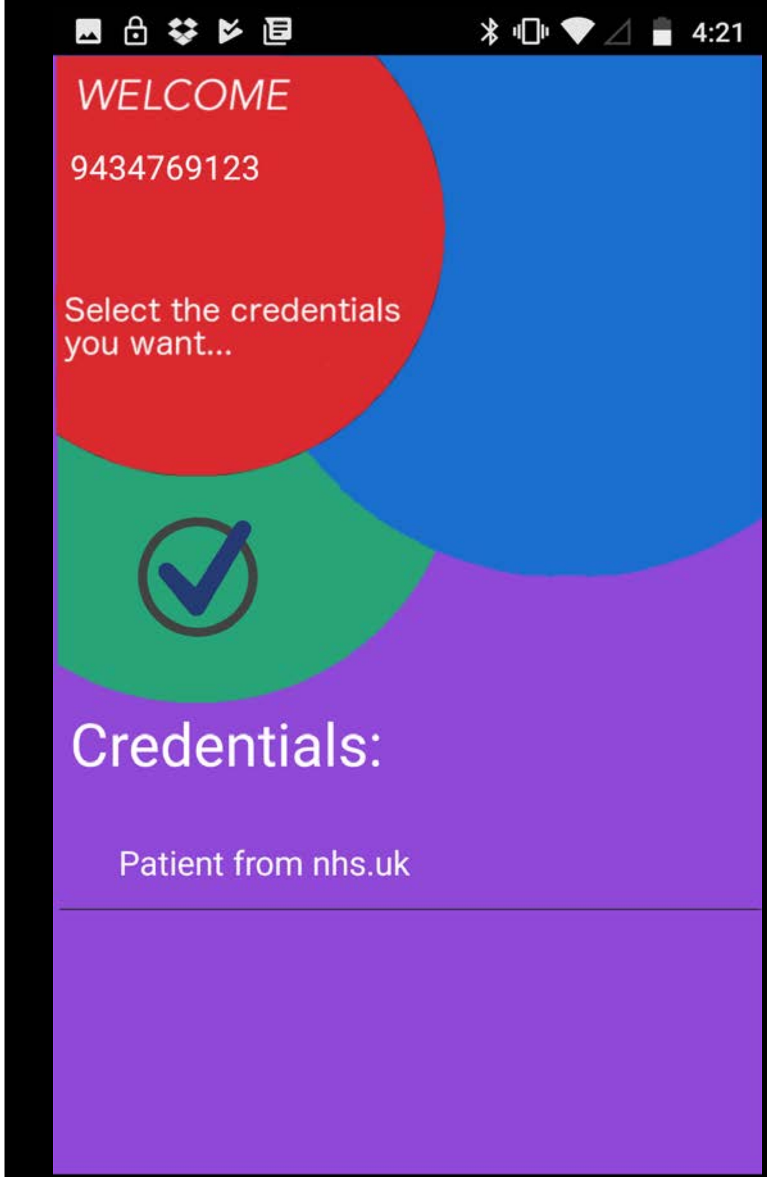
Registration Step 2. User authenticates to phone by swiping finger, phone creates a new key pair and sends public key to the NHS AA



Device Registration

Please register your device using your fingerprint.

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



WELCOME

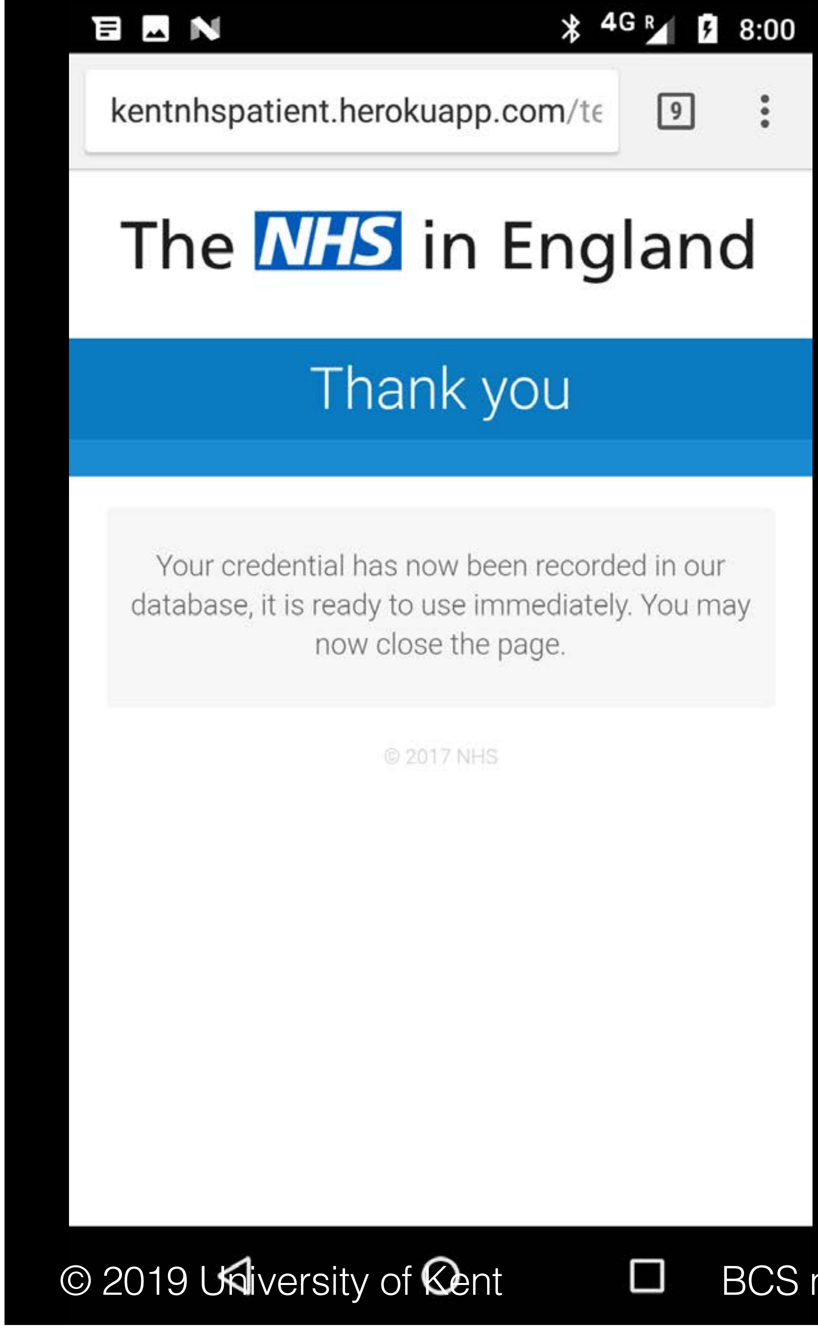
9434769123

Select the credentials you want...

Credentials:

Patient from nhs.uk

Registration Step 4. NHS confirms recording of credential



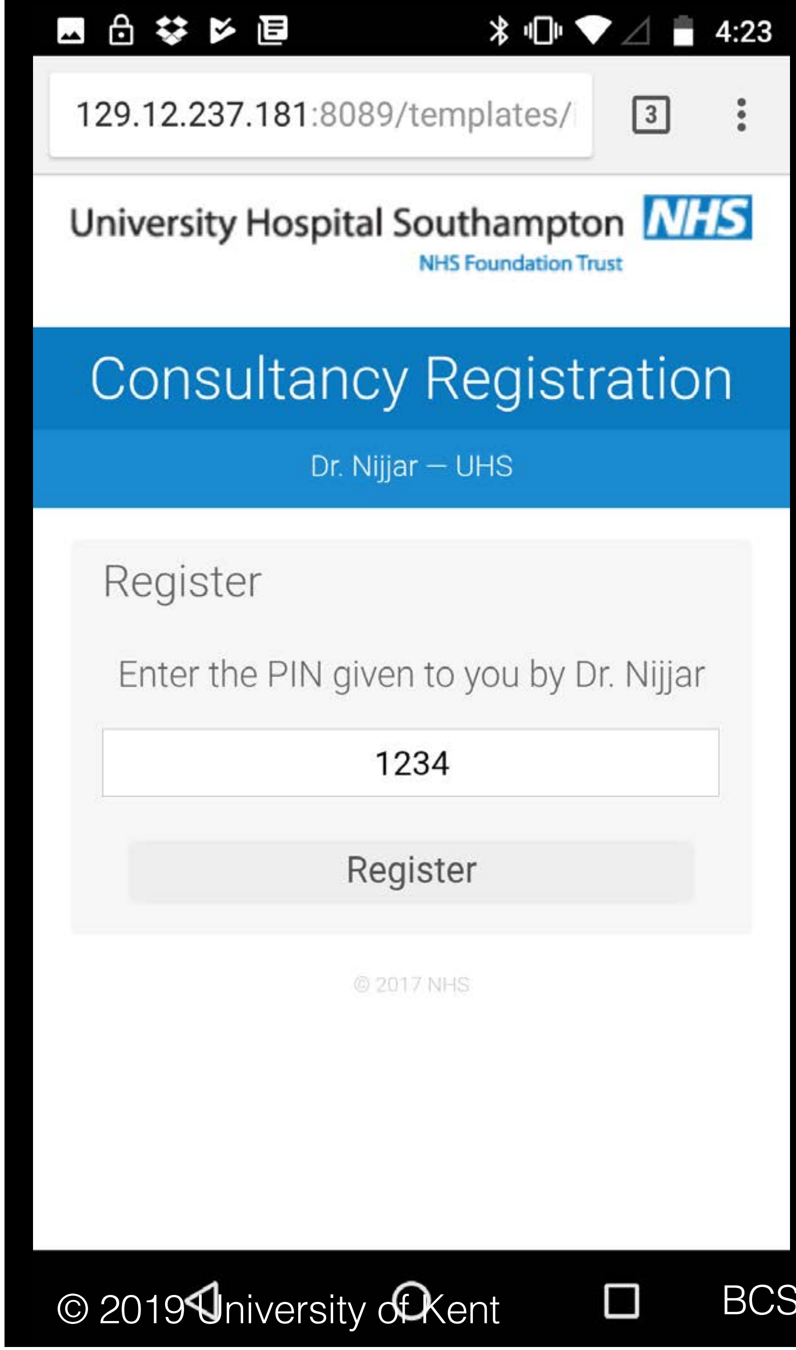
The NHS in England

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



4:23
129.12.237.181:8089/templates/
3
University Hospital Southampton NHS
NHS Foundation Trust

Consultancy Registration

Dr. Nijjar – UHS

Register

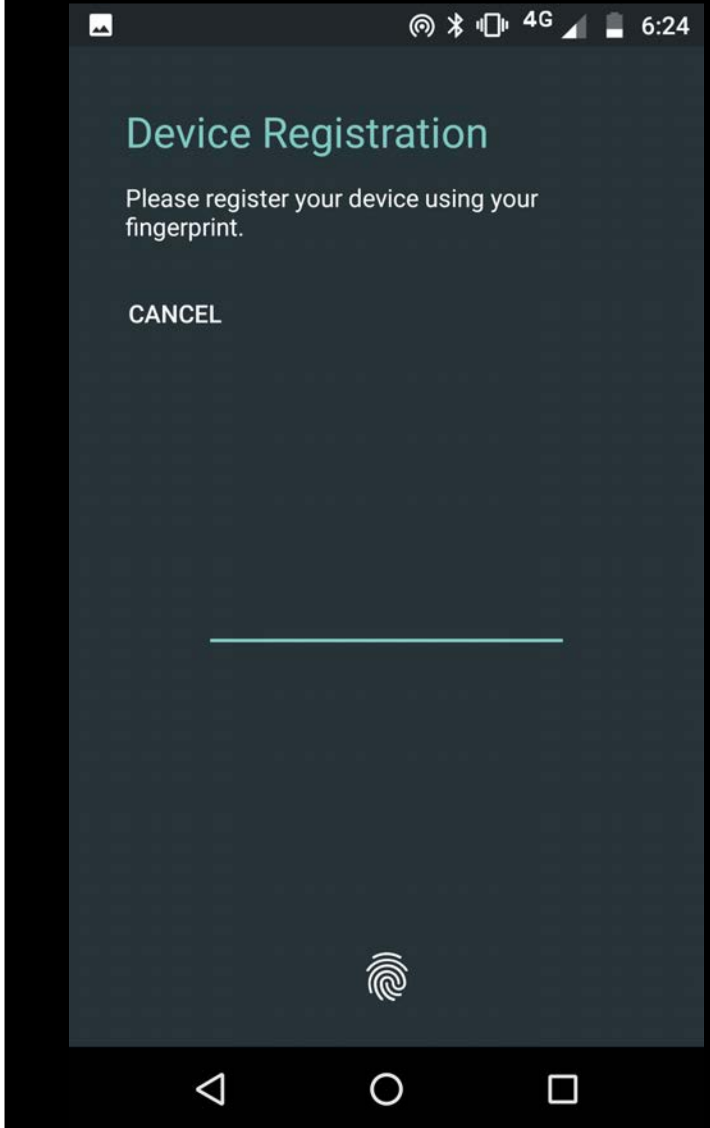
Enter the PIN given to you by Dr. Nijjar

1234

Register

© 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

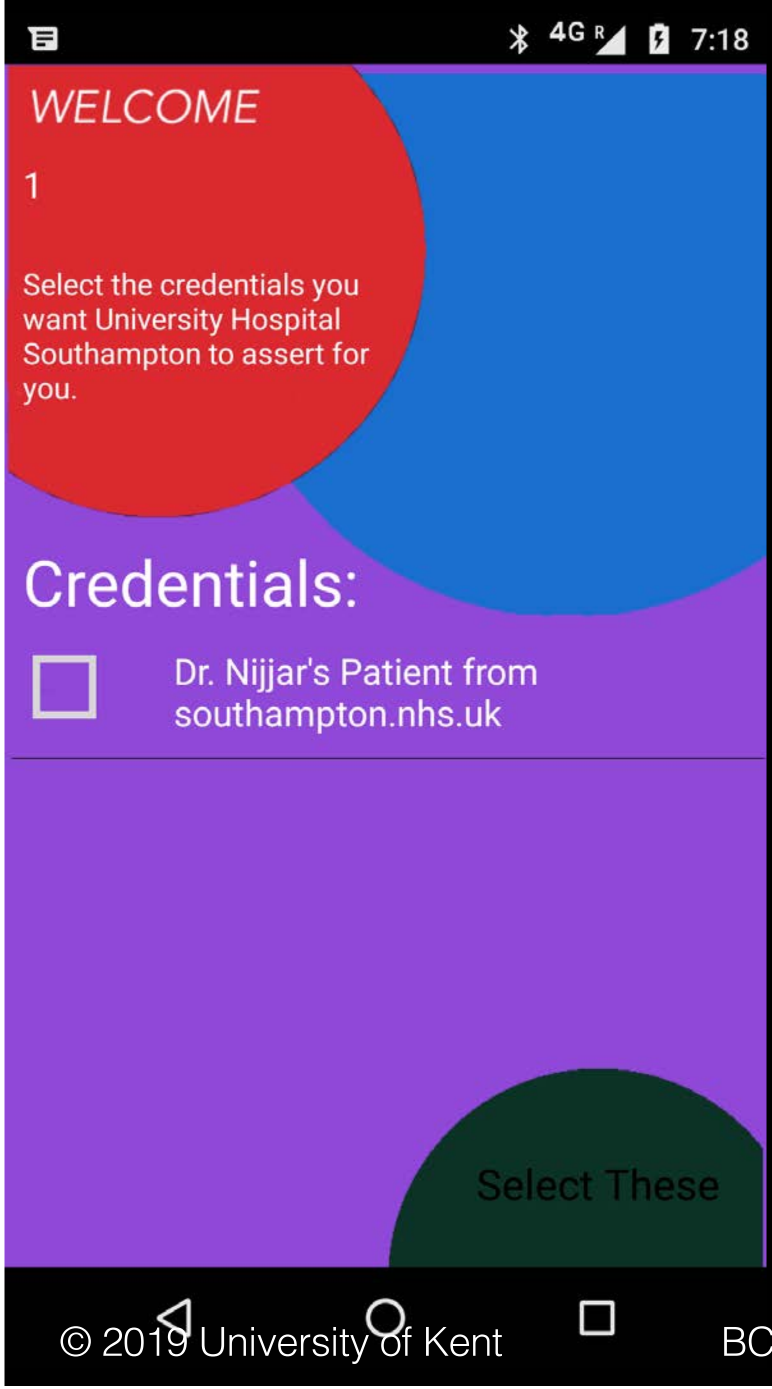


6:24

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

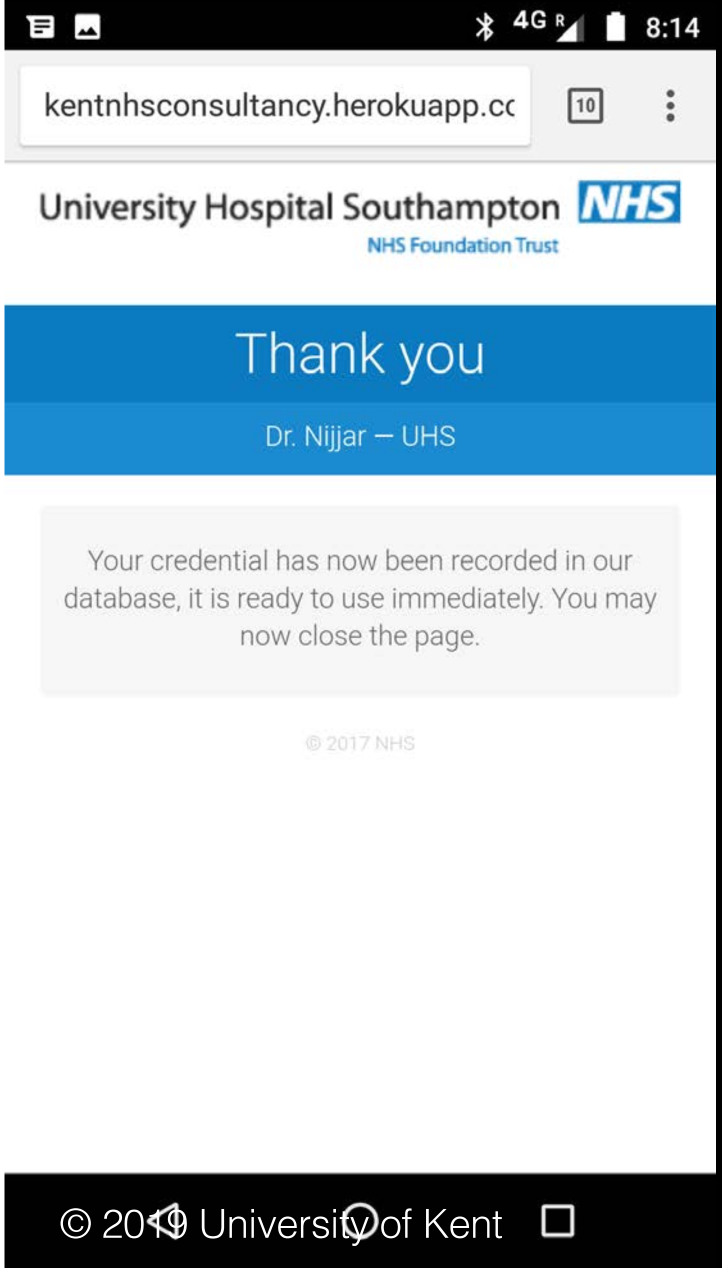
1

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

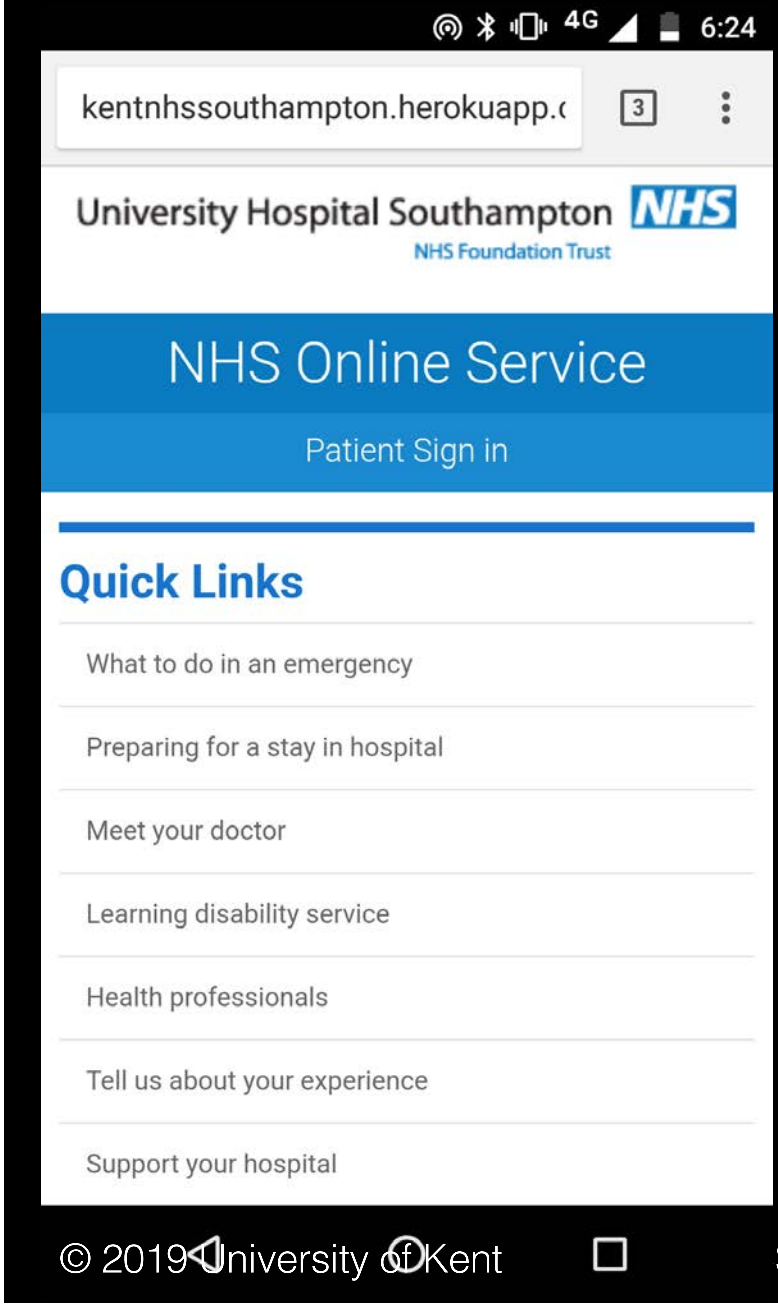

4G R
8:14
kentnhsconsultancy.herokuapp.cc
10
University Hospital Southampton NHS
NHS Foundation Trust

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.

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



University Hospital Southampton NHS
NHS Foundation Trust

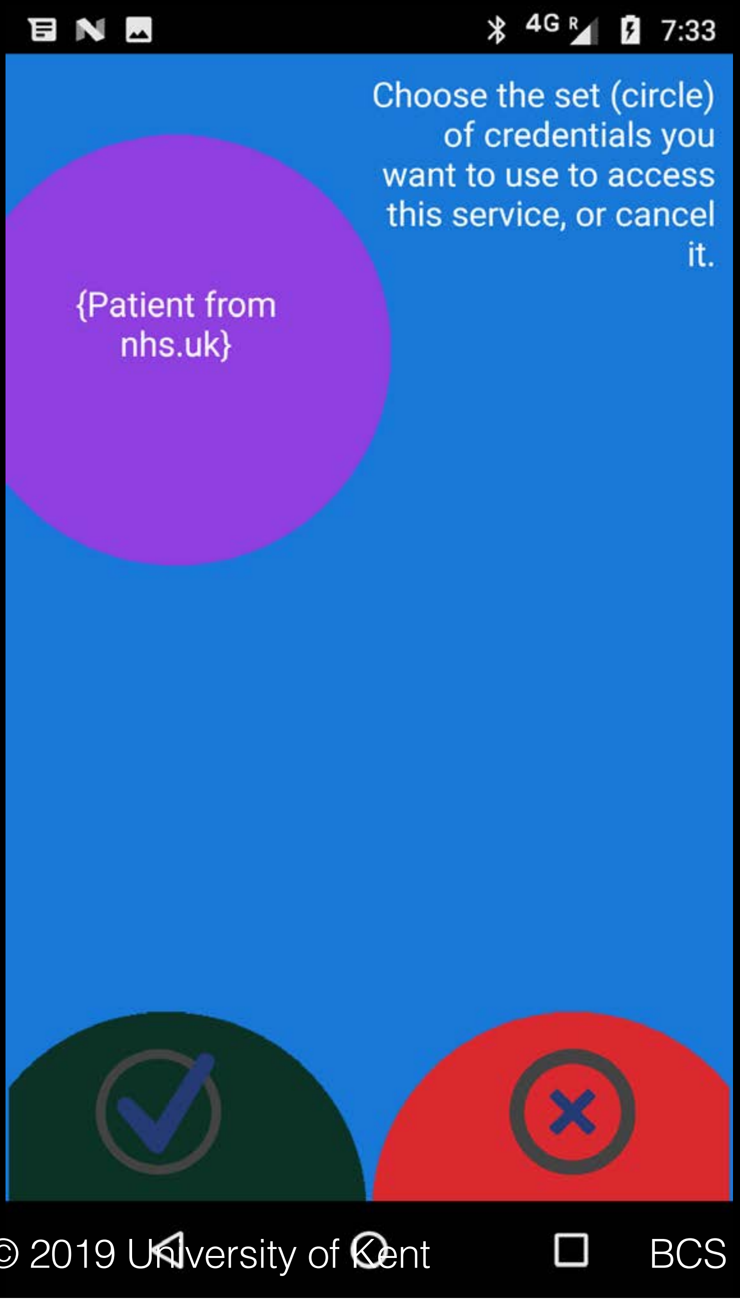
NHS Online Service

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

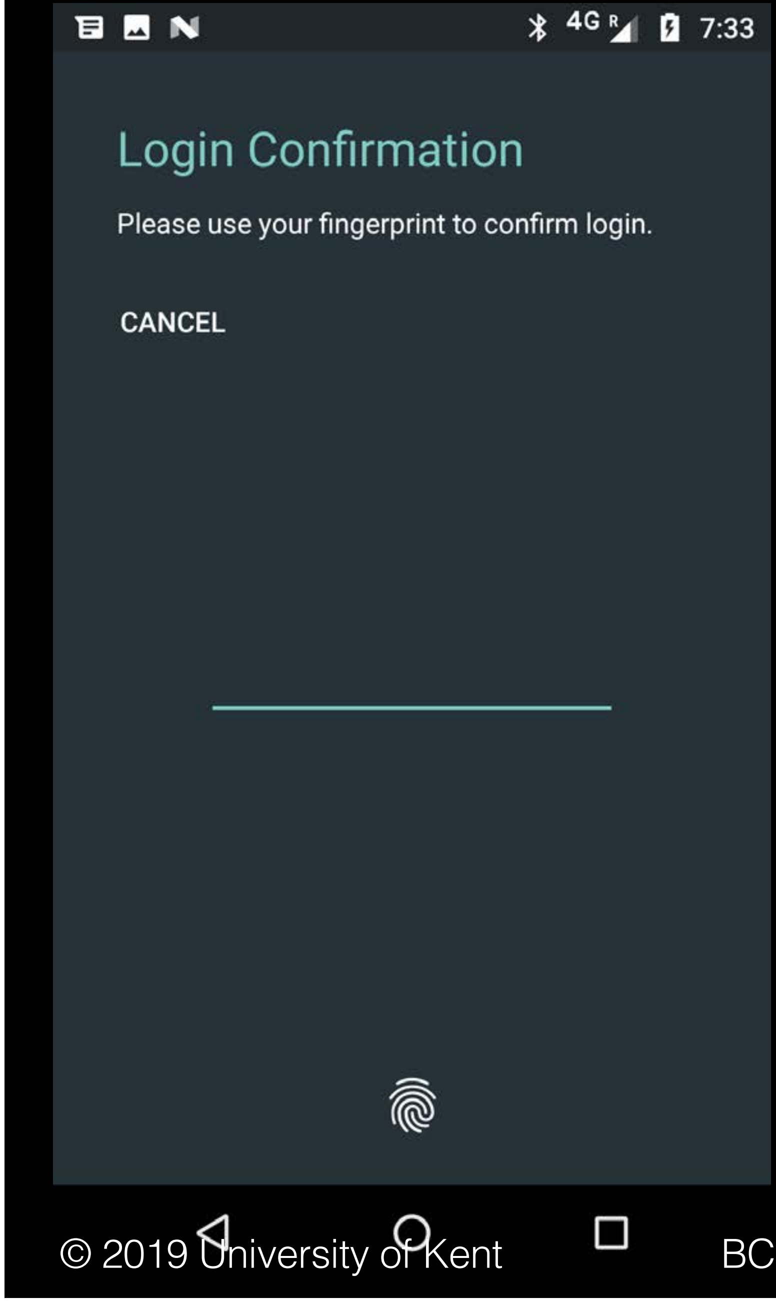
Use Step 2. Hospital sends its authz policy to the phone. Device matches policy against user's VCs and asks user to choose (no choice in this case)



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

{Patient from nhs.uk}

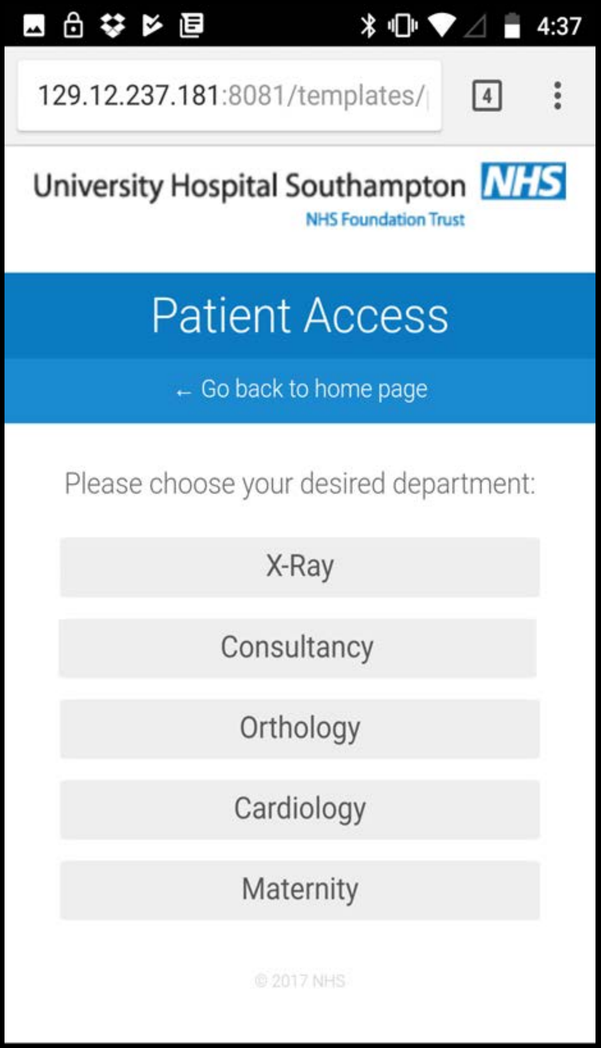
Use Step 3. User confirms selection with fingerprint



Login Confirmation

Please use your fingerprint to confirm login.

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

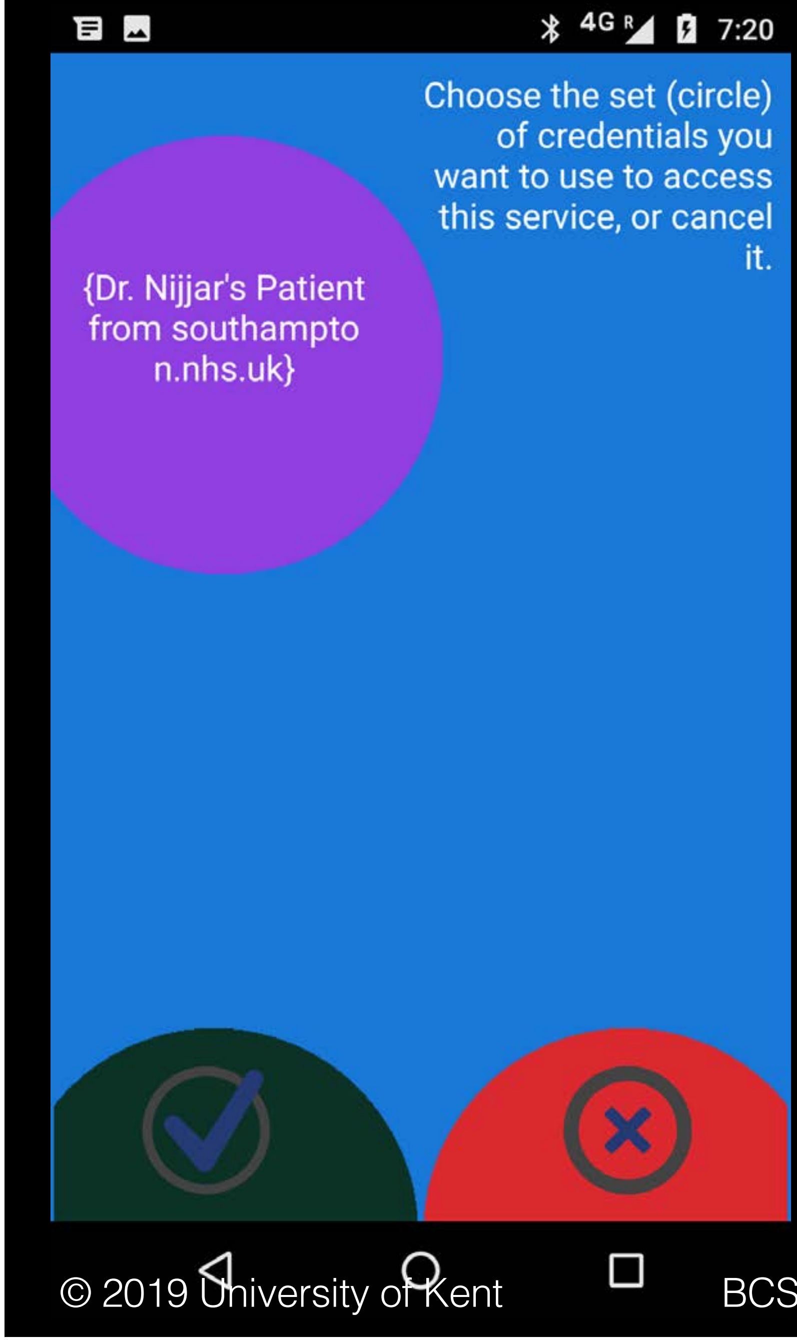
Orthology

Cardiology

Maternity

© 2017 NHS

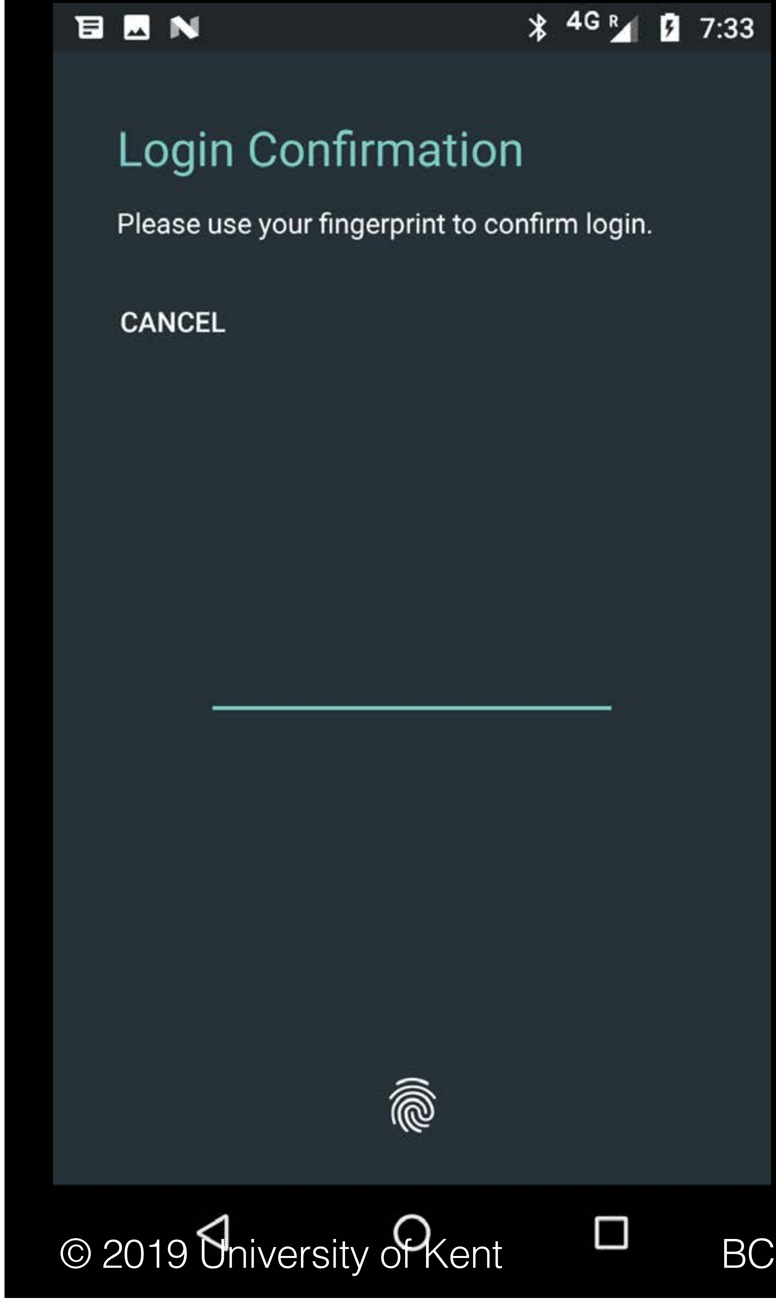
Use Step 5. Consultant's Authz policy is sent to phone. Phone matches policy against VCs on phone and asks user to choose (no choice in this case)



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}

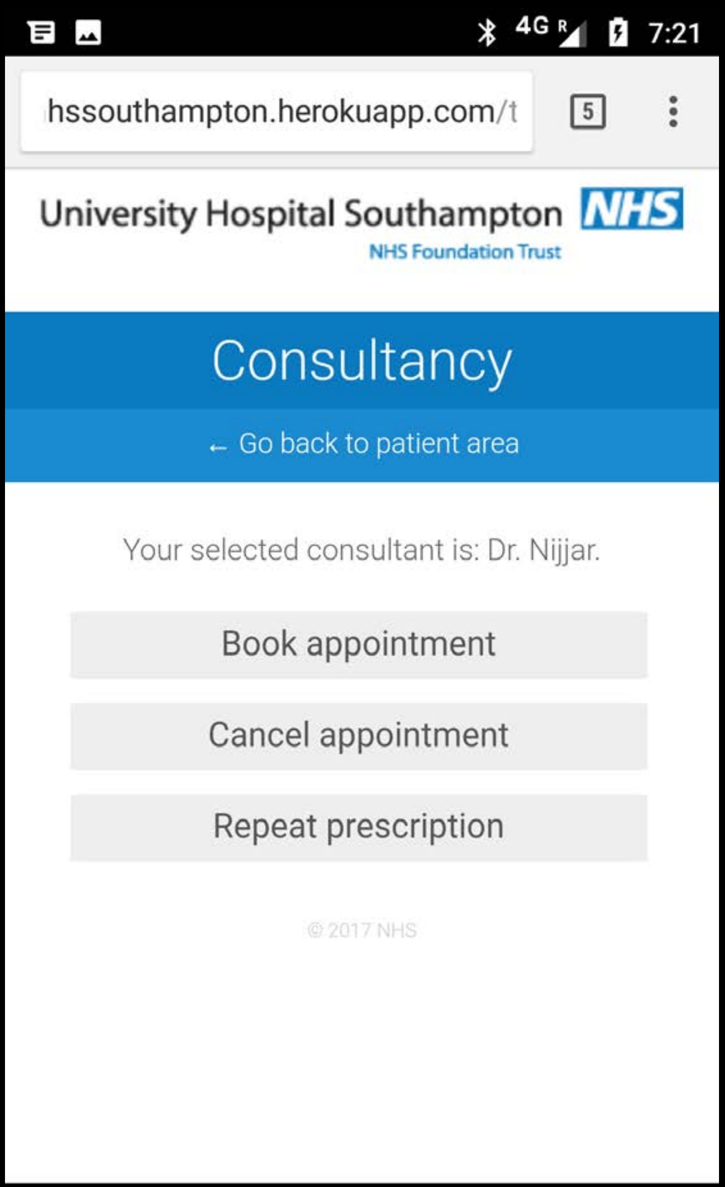
Use Step 6. User confirms selection with fingerprint



Login Confirmation

Please use your fingerprint to confirm login.

Use Step 7. Consultancy Menu is Displayed

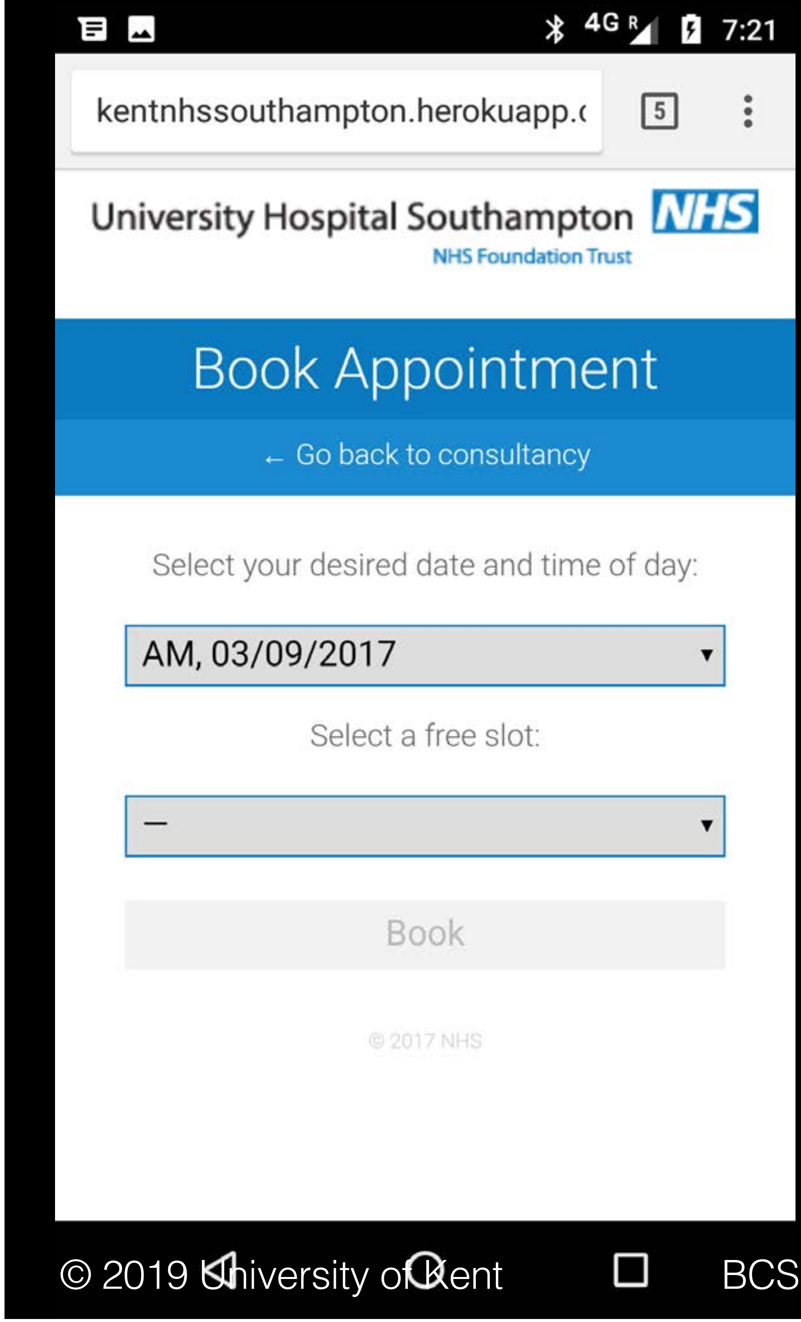


4G R
7:21
hssouthampton.herokuapp.com/t
5
University Hospital Southampton NHS
NHS Foundation Trust

Consultancy

Your selected consultant is: Dr. Nijjar.

Use Step 8. Book Appointment



7:21

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 ▾

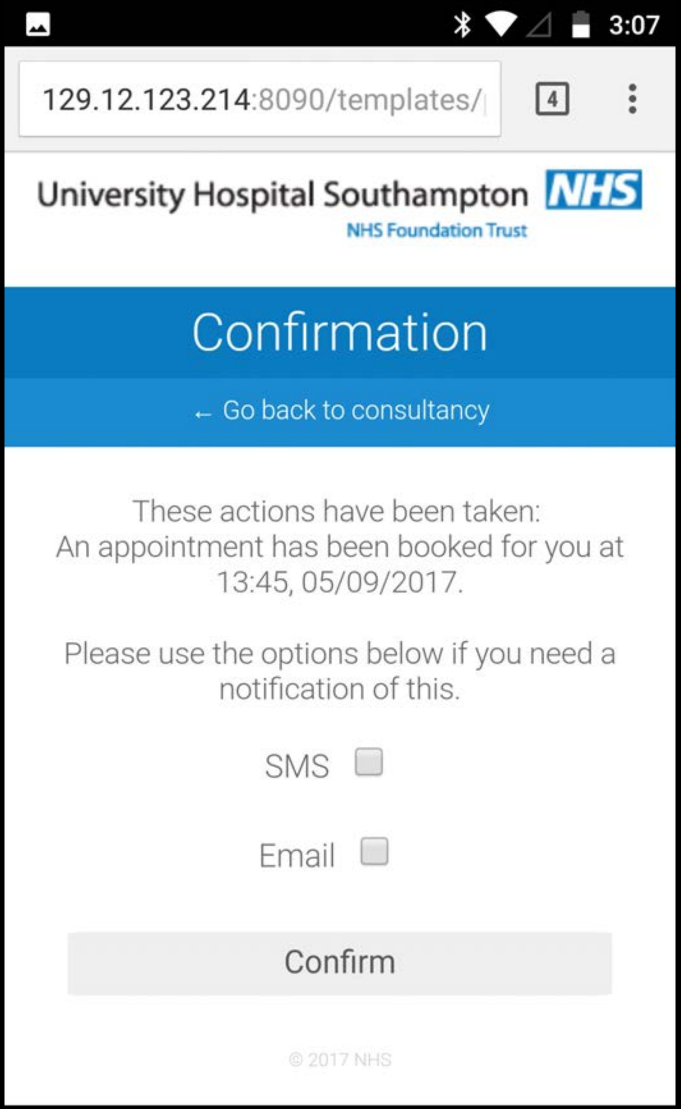
Select a free slot:

— ▾

Book

© 2017 NHS

Use Step 9. Confirmation Message



3:07

129.12.123.214:8090/templates/

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.

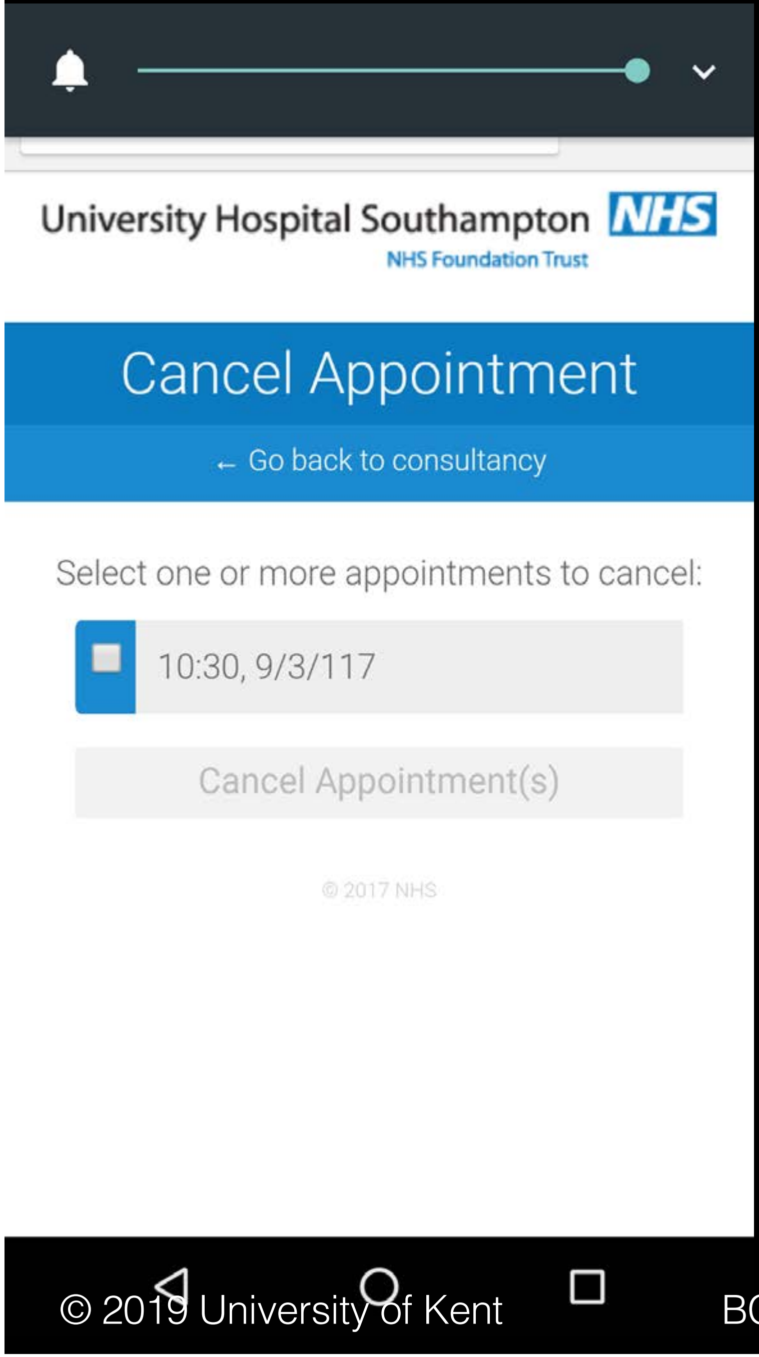
SMS □

Email □

Confirm

© 2017 NHS

Use Step 10. Cancel Appointment



University Hospital Southampton NHS
NHS Foundation Trust

Cancel Appointment

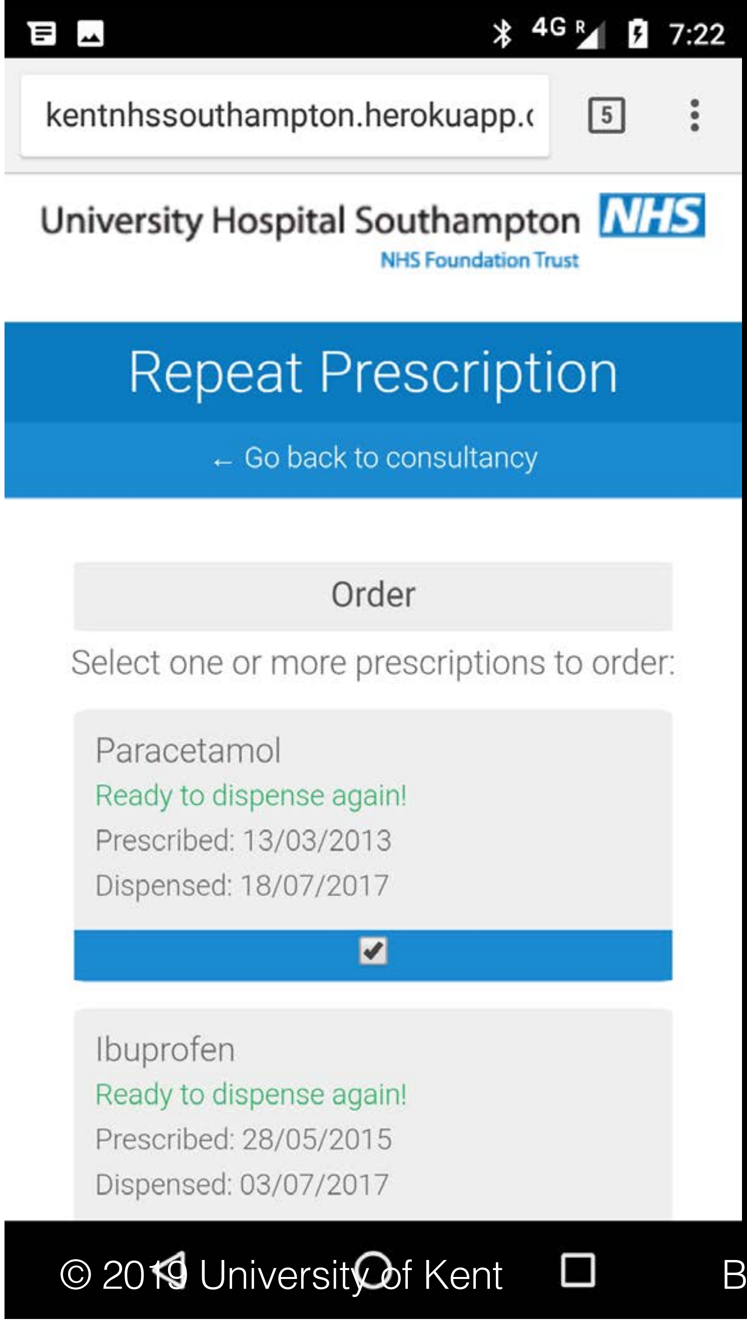
← Go back to consultancy

Select one or more appointments to cancel:

☐ 10:30, 9/3/117

© 2017 NHS

Use Step 11. Order Repeat Prescription



kentnhssouthampton.herokuapp.c

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

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 and have the potential to significantly reduce Identity Theft
    - Give the user full control of their identity
    - SP only obtains the attributes needed for identification and 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 because
    - No SP login passwords. Cryptographically protected credentials instead.
    - You would need to trick every IdP 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?