Improving Identity Management with W3C Verifiable Credentials

David W. Chadwick

Prof Information Systems Security

University of Kent

UK

Why is Identity Management Important?

“On the Internet, nobody knows you’re a dog.”

CartoonCollections.com

The True Cost of Identity Theft

Will NEVER be known!!

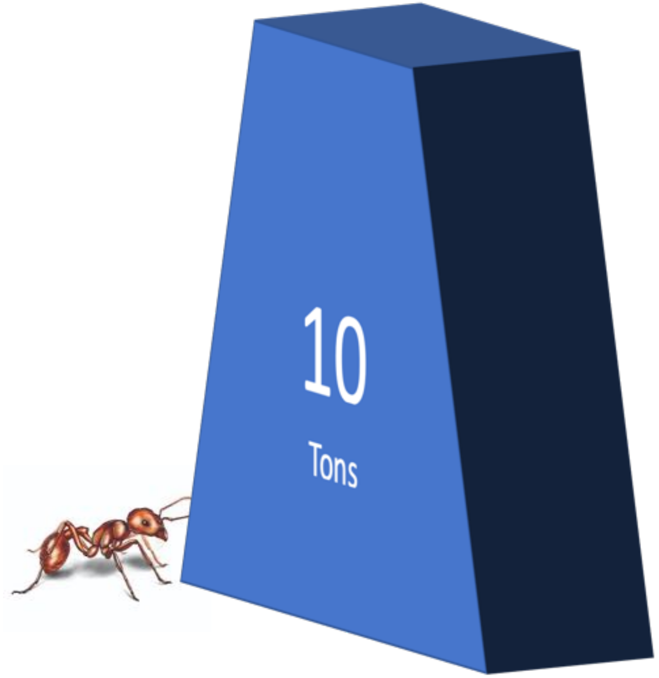
But we have some estimates

- **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**

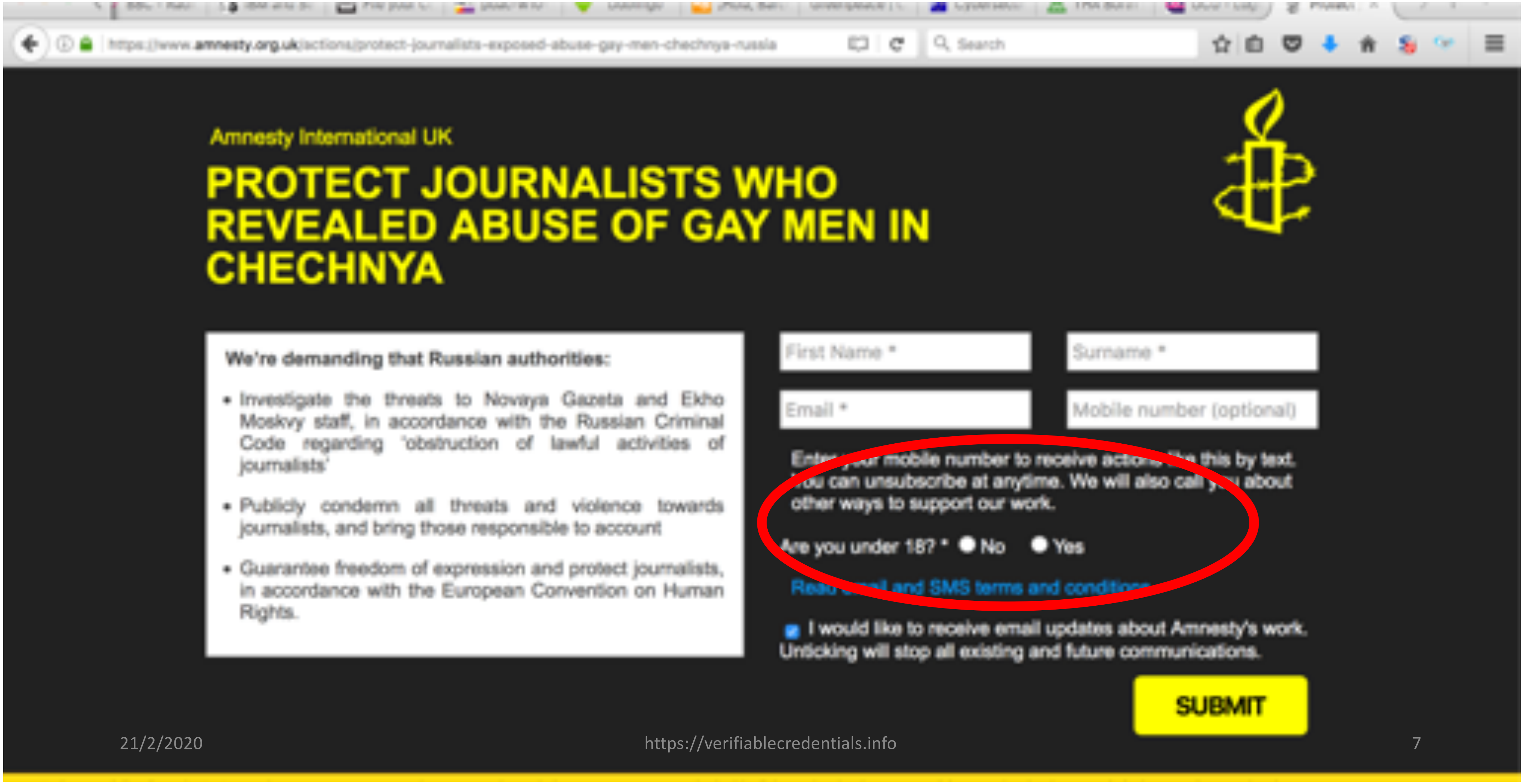
But we have some estimates

MASSIVE

Some attempts at Identity Management are Pathetic



Amnesty Petition – Are you under 18?



https://www.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.

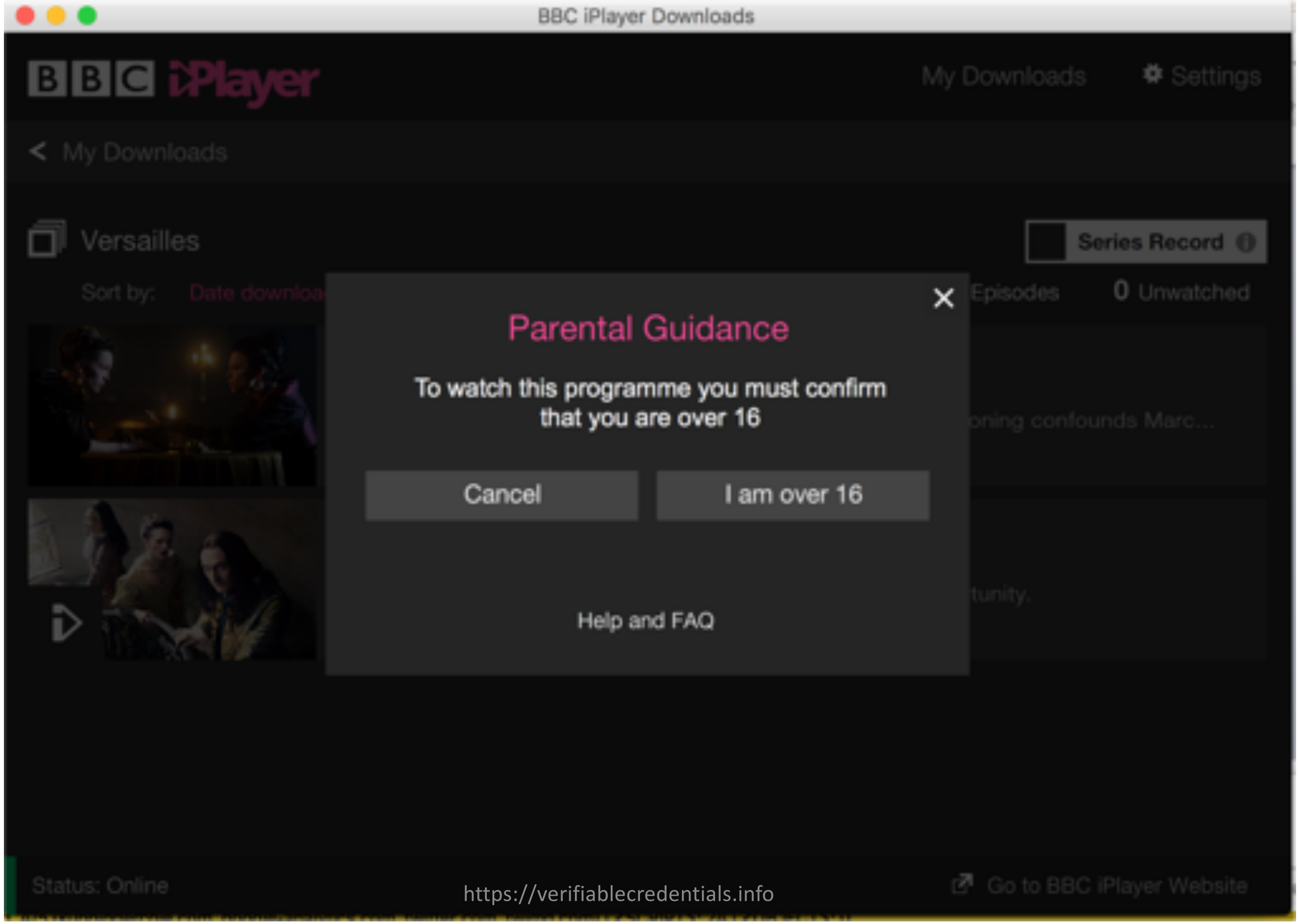
Are you under 18? * ○ No ○ Yes

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.

SUBMIT

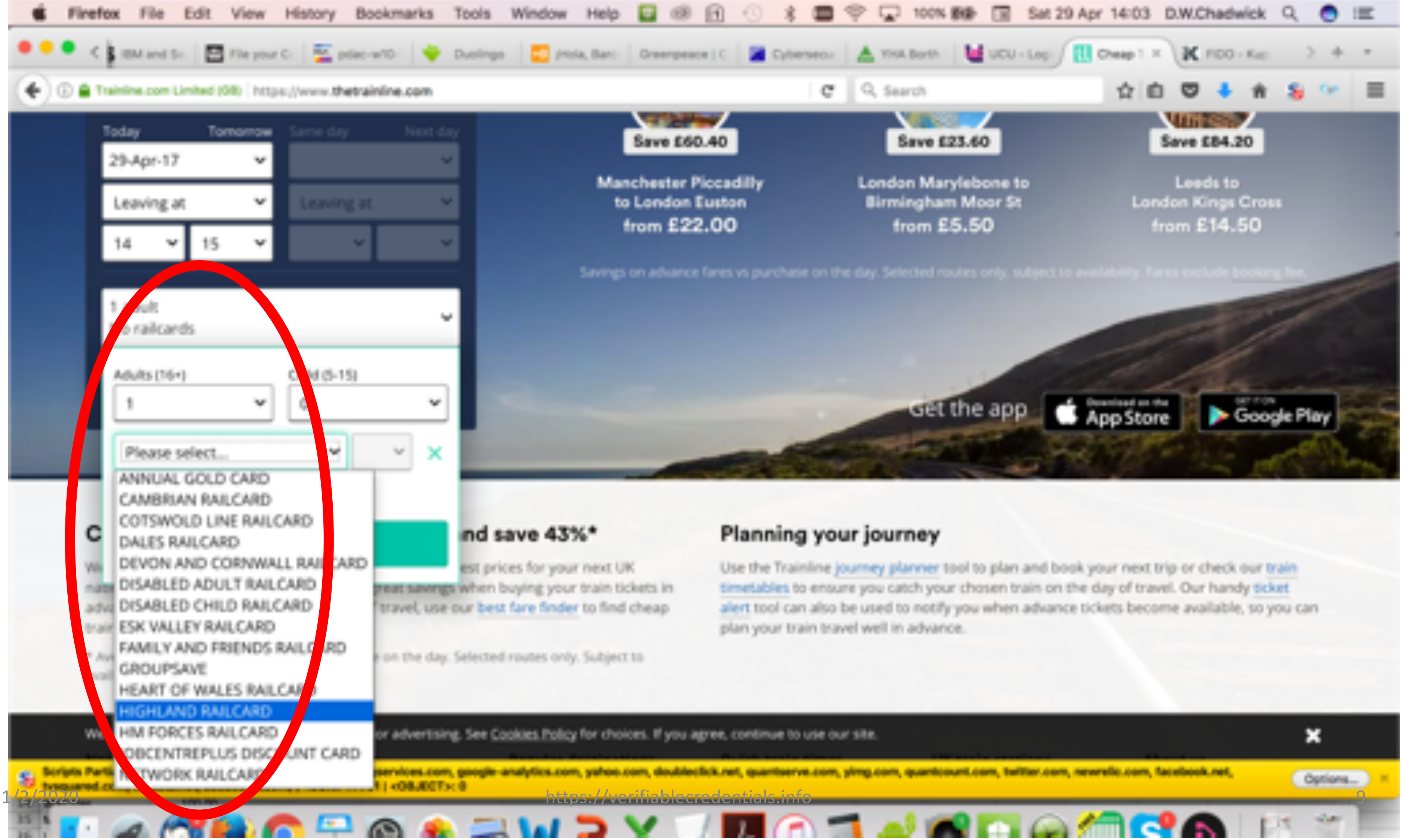
BBC – Parental Guidance



Parental Guidance

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

Purchase a reduced price train ticket with a Railcard



Firefox File Edit View History Bookmarks Tools Window Help
Sat 29 Apr 14:03 D.W.Chadwick
Trainline.com Limited (GB) https://www.thetrainline.com
Search

Today Tomorrow Same day Next day

29-Apr-17

Leaving at

14 15

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 fee.

Get the app App Store Google Play

...nd save 43%*

...est prices for your next UK ... great savings when buying your train tickets in ... travel, use our best fare finder to find cheap ...

... on the day. Selected routes only. Subject to

Planning your journey

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

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

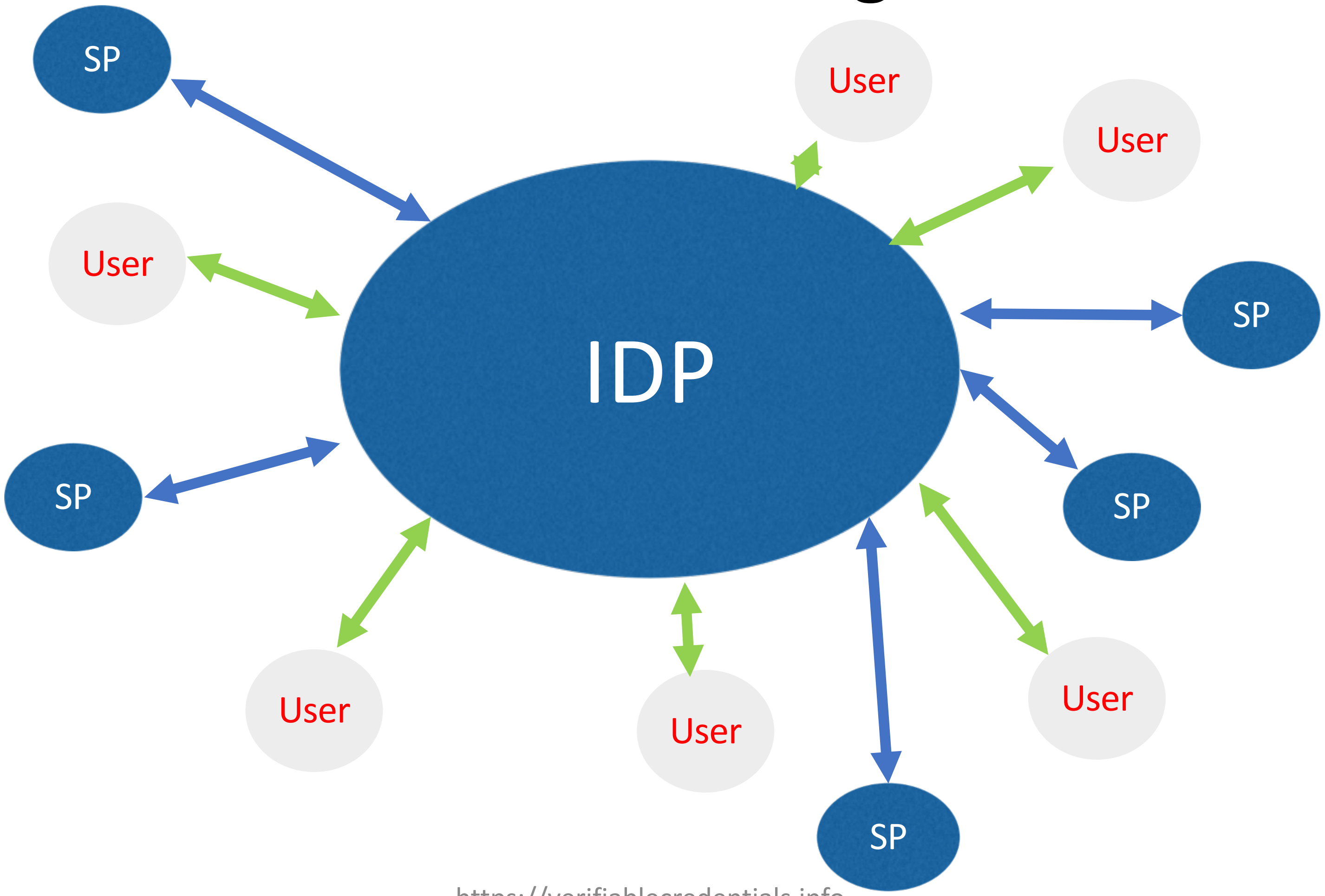
Existing Federated Identity Management Products

- Are also pathetic in many respects

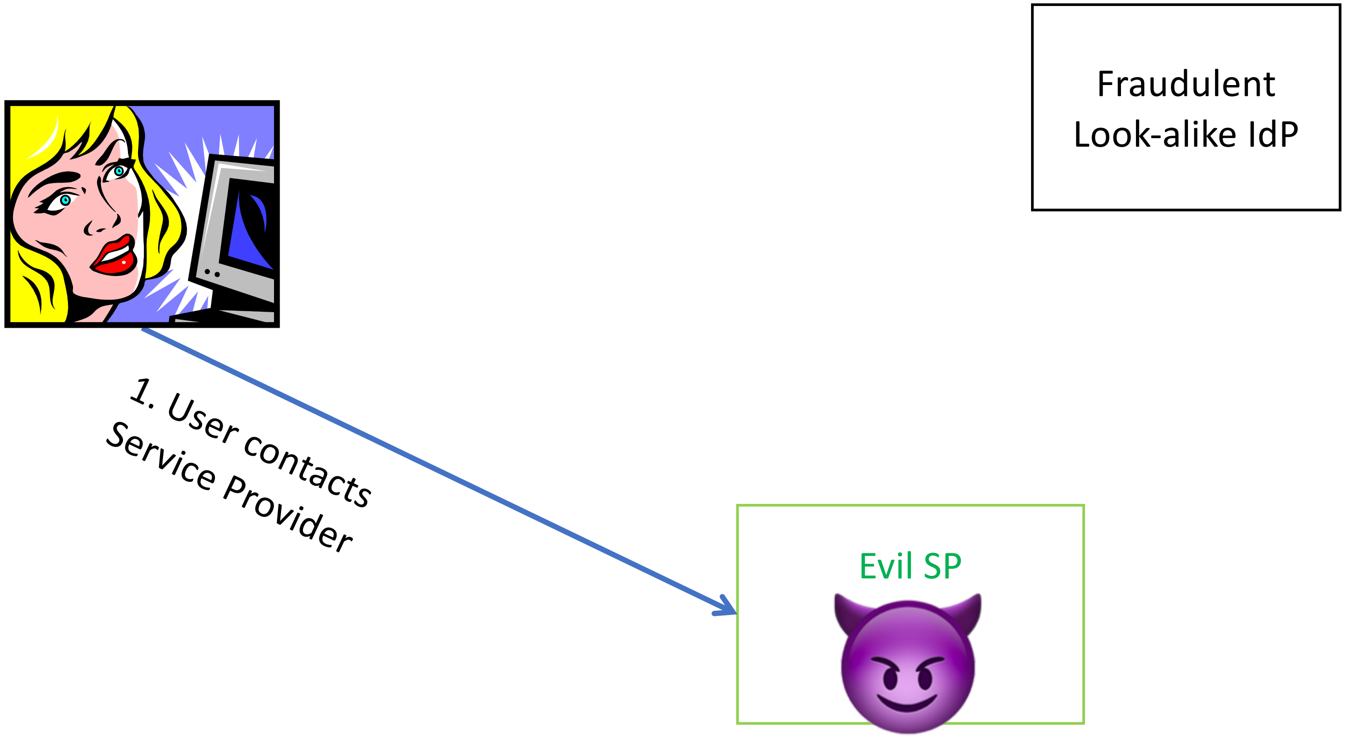
They place the Identity Provider at the Centre of the Identity Ecosystem

- Makes IdPs too powerful. They control which Service Providers the users can log into
- This violates the user’s privacy as the IdP knows every SP the user contacts and when

Federated Identity Management
The IdP is King



FIM systems are Susceptible to Phishing attacks

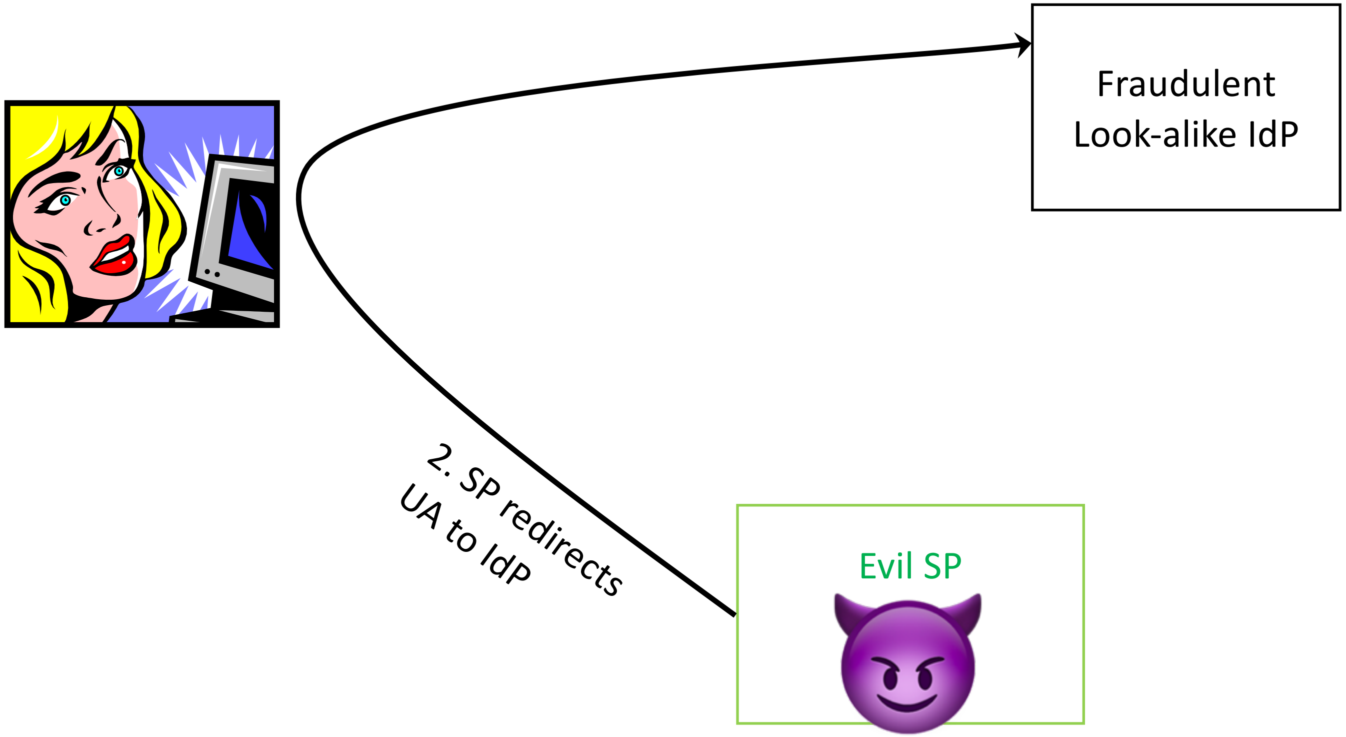


Fraudulent Look-alike IdP

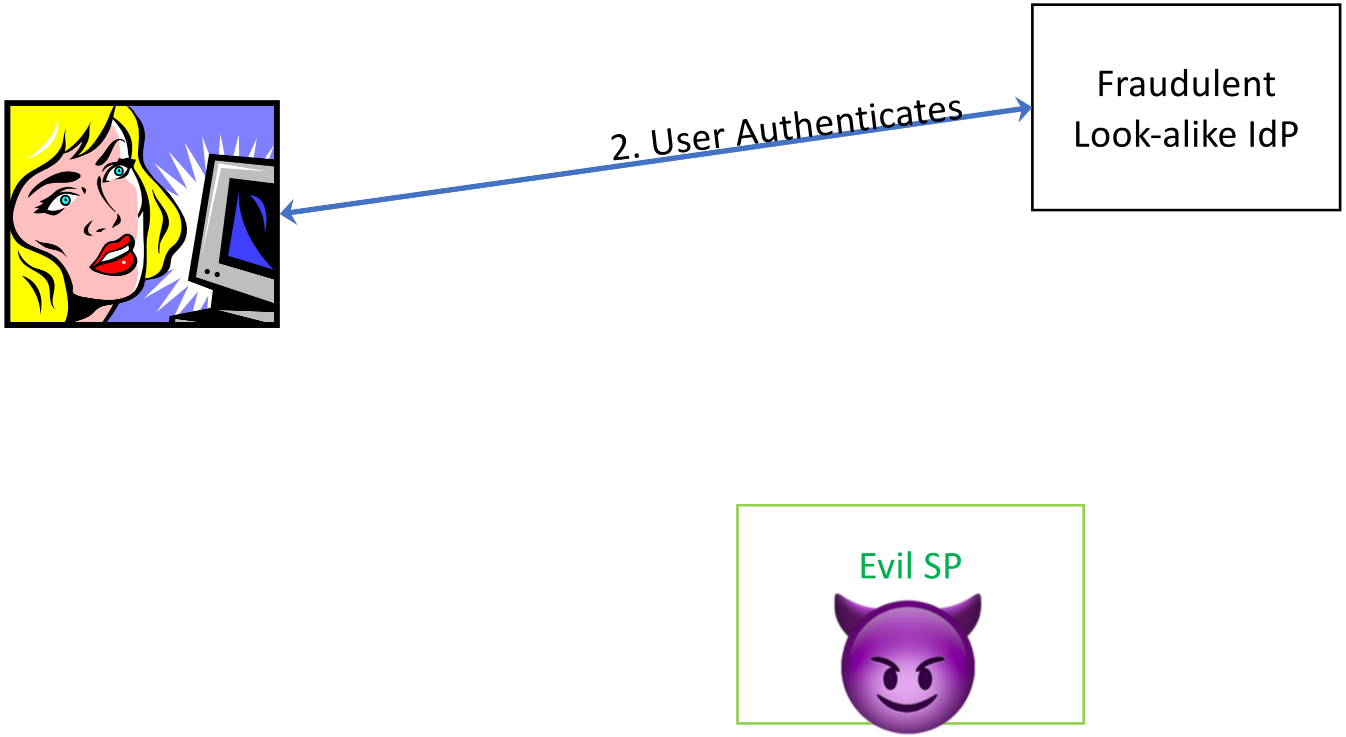
1. User contacts Service Provider

Evil SP

FIM systems are Susceptible to Phishing attacks



FIM systems are Susceptible to Phishing attacks



2. User Authenticates

Fraudulent Look-alike IdP

Evil SP

FIM systems are Susceptible to Phishing attacks

Fraudulent
Look-alike IdP

Evil SP
😈

IdPs unwilling or unable to release the identity attributes the SPs require

- “Insufficient attribute release by IdPs is considered by user communities as the major problem today in the eduGAIN space”
  - EU AARC Project Deliverable DNA2.4 “Training Material Targeted at Identity Providers” 27 July 2016

IdPs are Honeypots

- Attacking them can provides access to all the users' SP accounts
- Sept 2018. Facebook hacked, and 50m user accounts were possibly compromised
  - https://www.theguardian.com/technology/2018/oct/02/facebook-hack-compromised-accounts-tokens
- Feb 2020. Facebook Hacked and confirmed 13.4 Million Follower Twitter Accounts were compromised

Trust model is wrong

- IdPs have to trust SPs, in order to comply with GDPR, since they are releasing the user’s personal information to the SP

Imagine

- A world in which users have dozens of plastic cards
- Which they carry around in their wallets and use them to gain access to services and resources
- Not Difficult
- And the user has to contact each card issuer before they can show the card to anyone
- Pathetic!
- But this is the FIM world today

What are W3C 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)
- Can be used as Authorisation tokens in Attribute Based Access Control (ABAC) systems

Compare FIM assertions to Plastic Cards, Passports etc.

- Users can only show their credentials to SPs that the IdP trusts
- The IdP knows which SPs the user is visiting and controls this
- Normally the IdP has to provide **all** the credentials that the SP requires
- Credentials are short lived so not revocable
- Susceptible to phishing attacks
- THE IDP IS IN CONTROL

- Users can show their cards to any SPs that they trust
- The issuer is not aware of the SP, nor able to stop the user visiting it
- Users can aggregate their cards as required by the SPs
- Cards are long lived and users can ask issuers to revoke their cards on demand
- Not susceptible to phishing attacks
- USERS ARE IN CONTROL

Take Home 1. 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
- Because DAVOS says so!

This is exactly what W3C VCs do

“Users who own their own digital identity”

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

“User empowerment through user control of what data they share, improving their experiences across their digital context”

Community Paper

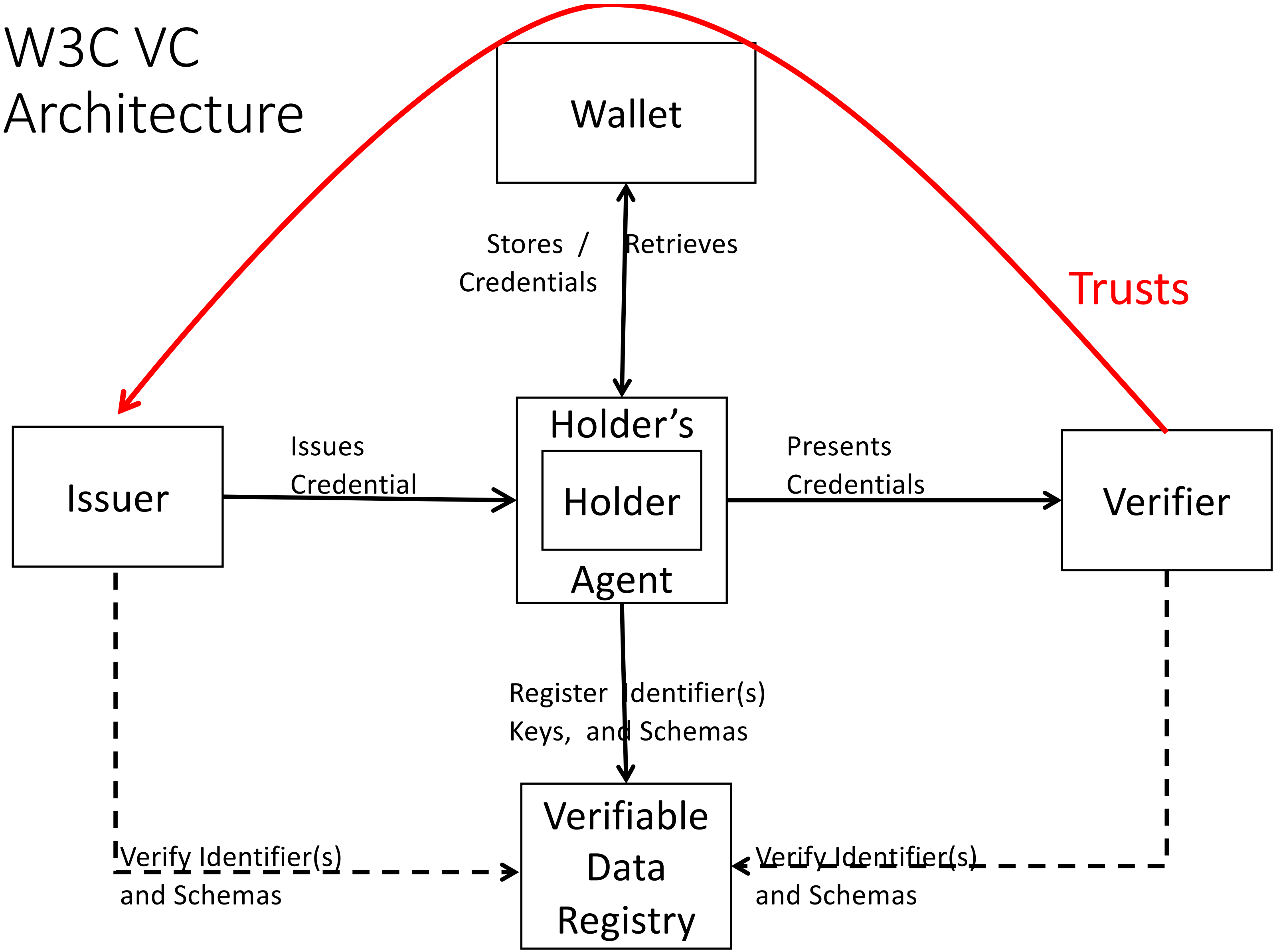
Reimagining Digital Identity:
A Strategic Imperative

“High degree of trust, reliability, and security across the value chain in digital transactions based on trusted digital identity”

“High level of value made possible through interoperability across domains and use cases”

January 2020

W3C VC Architecture



Take Home 2

- W3C Verifiable Credentials DO NOT NEED Distributed Ledger Technologies
- DLTs do not need W3C VCs
- But
- They may be combined together synergistically

W3C 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. Standard examples are JWT/JWS and LD-Proofs
- Protocols are out of scope of W3C VC WG
- WG finished, Recommendation published in November 2019
- VC Working Group is now recharted in maintenance mode
- DID WG started 1 October 2019 to standardize the DID URI scheme, and the data model and syntax of DID Documents
- Credentials Community Group is continuing to progress VC issues such as possible extensions, possible protocols, schemas, implementation issues etc

A Minimal 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

- JSON-LD construct used to map globally unique URIs into user friendly aliases
  - E.g. "VerifiableCredential” instead of "https://www.w3.org/2018/credentials#VerifiableCredential",

- 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 as in LDAP / MS AD e.g. is my ‘telno’ the same as your ‘telno’ or her ‘telephone_number’

A Maximal VC ? – there is no maximum

```
{
        "@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"} },
        "termsOfUse": [{"type": "IssuerPolicy"}],
        "nonTransferable": "True",
        "credentialStatus": {
                "id": "https://example.edu/status/24",
                "type": "CredentialStatusList2017"},
        "credentialSchema": {"id": "https://example.org/examples/degree.json",
                "type": "JsonSchemaValidator2018"},
        "refreshService": {"id": "https://example.edu/refresh/3732",
                "type": "ManualRefreshService2018"},
        "evidence": {"type": "DocumentVerification"},
        "myExt1": {"type": "DefinedByMe"},
        ”yourExt1": {"type": "DefinedByYou"},
        "proof": {}
}
```

A Verifiable Presentation

```
{
        "@context": ["https://www.w3.org/2018/credentials/v1"],
        "id": "urn:uuid:3978344f-8596-4c3a-a978-8fcaba3903c5",
        "type": ["VerifiablePresentation"],
        "verifiableCredential": [{ }],
        "proof": {}
}
```

VC Proof Mechanisms

- No Single Mandatory Cryptographic Proof Mechanism is Standardised
- Three Proof mechanisms are described
- Jason Signatures JWT/JWS
- JSON-LD Signatures
- Zero Knowledge Proofs (such as Anonymous Credentials)

Implementing a VC Ecosystem

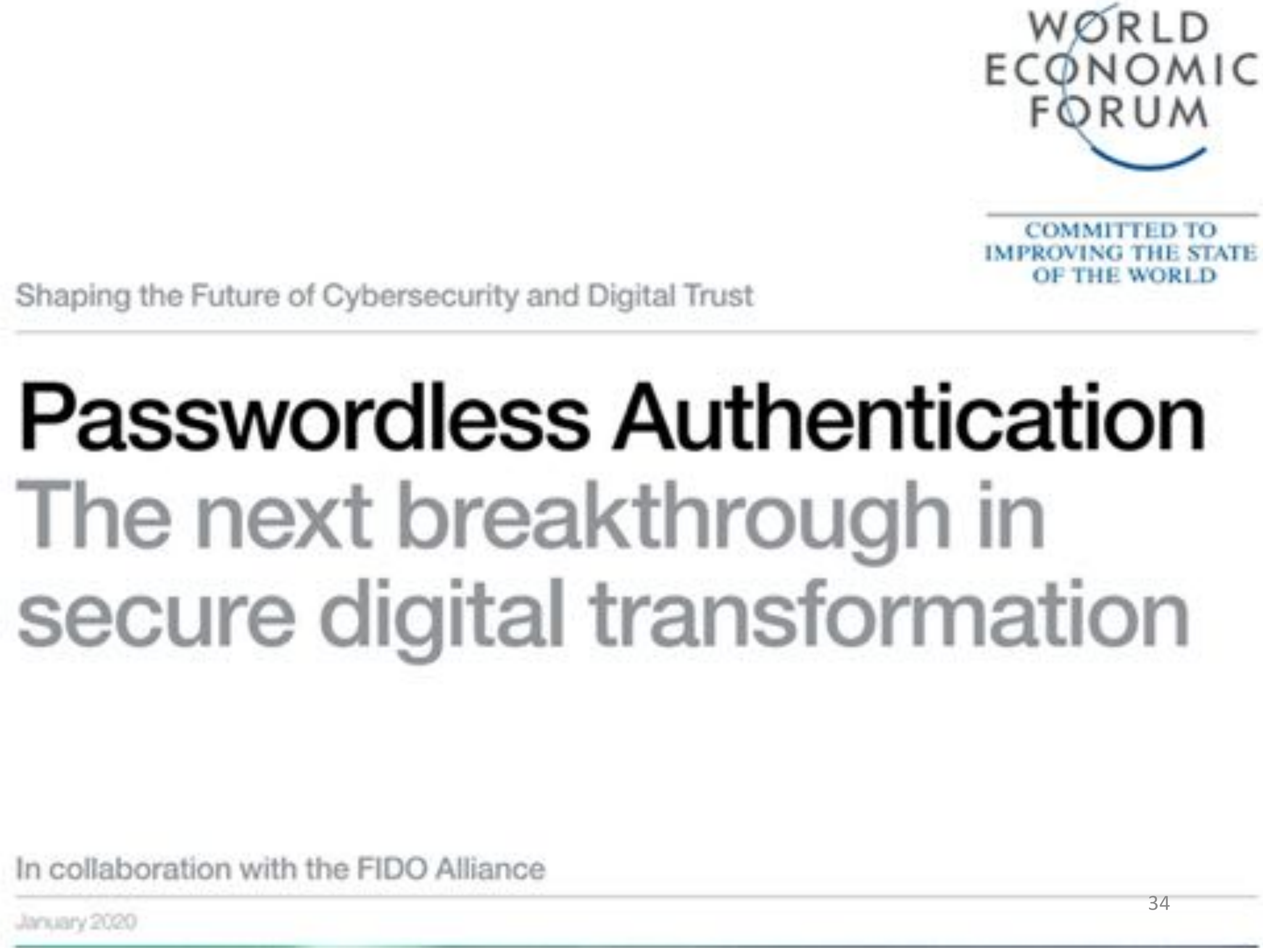
- Since there are no standard protocols yet for VCs we originally defined our own based on FIDO

- This is described here

David W Chadwick, Romain Laborde, Arnaud Oglaza, Remi Venant, Samer Wazan, Manreet Nijjar “Improved Identity Management with Verifiable Credentials and FIDO” to be published in IEEE Communications Standards Magazine Dec 2019 (??)

- And our latest prototype is based on FIDO2 - what the World Economic Forum 2020 says is the next breakthrough in security

We use FIDO2



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

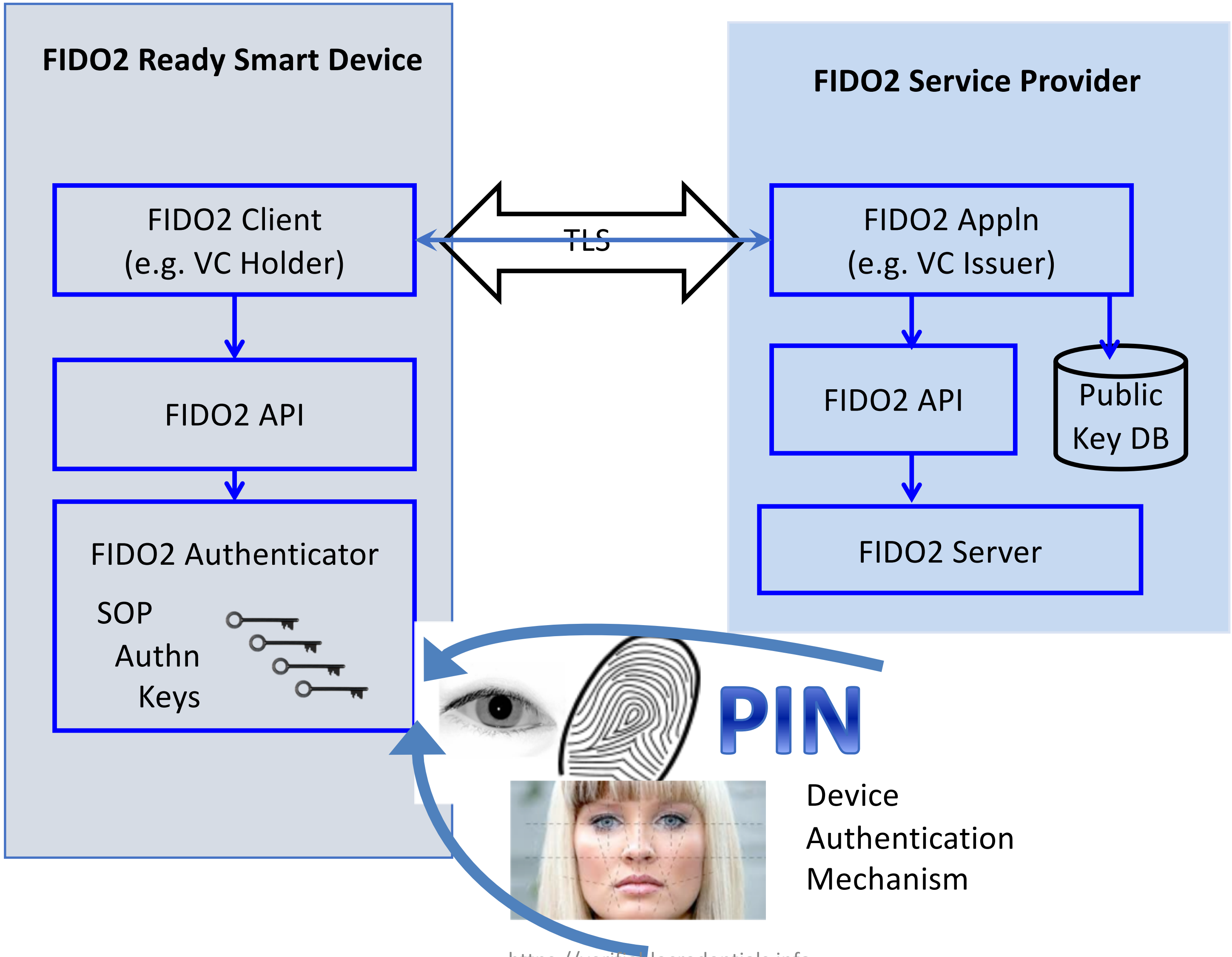
Passwordless Authentication
The next breakthrough in secure digital transformation

In collaboration with the FIDO Alliance

January 2020

Fast Identity Online - FIDO

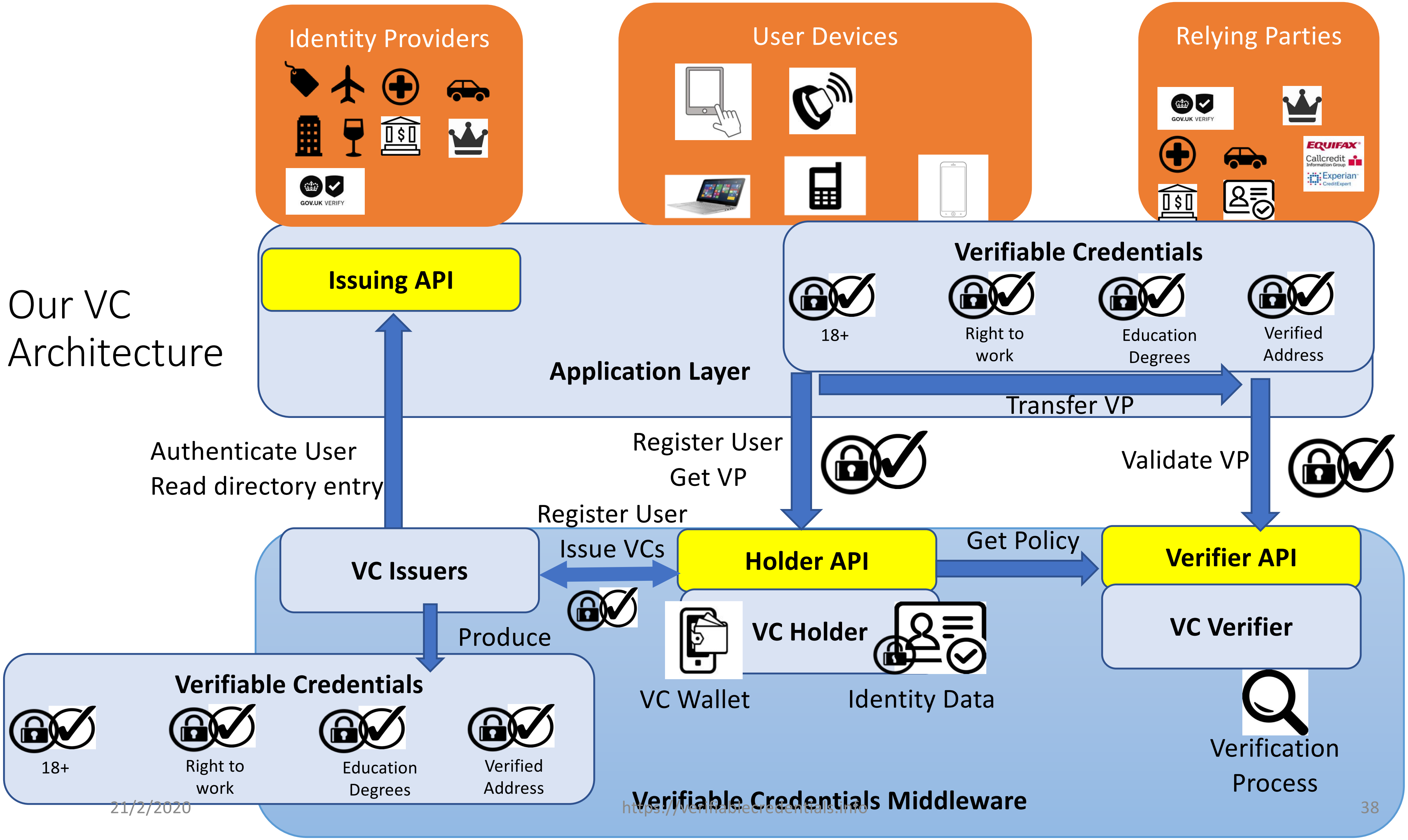
- The FIDO Alliance developed the original FIDO specifications for strong authentication in 2014
- Then took them to W3C for standardization, which published the Web Authentication Recommendation in 2019 (FIDO2)
- Uses asymmetric encryption, with a unique key pair created for every web site the user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


FIDO2 Ready Smart Device
FIDO2 Client
(e.g. VC Holder)
FIDO2 API
FIDO2 Authenticator
SOP
Authn
Keys
TLS
FIDO2 Service Provider
FIDO2 Appln
(e.g. VC Issuer)
FIDO2 API
Public
Key DB
FIDO2 Server
PIN
Device
Authentication
Mechanism

BUT…

- FIDO only provides strong authentication
- It does not identify the user or provide for fine grained authorisation
  - which are the main goals of W3C verifiable credentials
- So… we devised an identification and authorisation enhancement for FIDO2 using the W3C verifiable credentials data model

Our VC Architecture



Identity Providers

User Devices

Relying Parties

Issuing API

Application Layer

Verifiable Credentials

18+

Right to work

Education Degrees

Verified Address

Transfer VP

Authenticate User
Read directory entry

Register User
Get VP

Validate VP

Register User

Issue VCs

Get Policy

VC Issuers

Holder API

Verifier API

VC Holder

VC Verifier

Produce

VC Wallet

Identity Data

Verification Process

Verifiable Credentials

18+

Right to work

Education Degrees

Verified Address

Verifiable Credentials Middleware

Three Easy To Use APIs

- These allow any application to easily integrate W3C FIDO2 and VCs into their application to provide
    - Strong Authentication
    - Strong Identification
    - Strong Authorisation
- All defined in YAML and publicly available

VC Holder API

- POST /v1/register - Register with an Issuer

  { "authnCreds": { },
  "vcIssuer": "<URL of the VC Issuer”
  }
  Returns OK or an Error

- POST /v1/reregister - Re-register with the Issuer
- POST /v1/getVP

  { "authnCreds": { },
  "policyMatch": { },
  "sp": "<URL of resource/service user wants to access",
  "vcVerifier": "<URL of the SP’s VC Verifier>"
  }
  Returns a VP in JWT format

VC Issuer API

- POST /authenticate   - authenticate the user

  {"authnCreds": {}

  }

  Returns

      {"userHandle": "adfasdasfadsfdsa",
       "username": "fred"
      }

- GET /getAllAttrs/{userHandle}   - get all the user’s identity attributes

  Returns

  [

  {<user atts for one VC>}

  ]

VC Verifier API

- POST v1/decision   - Request an Access Decision

```
{ "atts": true|false,
  "policyMatch": { },
  "vpjwt": "eyJ1c2VybmFt……Y2RlZiJ9fQ==”
}
Returns
 {"atts": {},
"authnCreds": {},
"granted": true|false}
```

- POST v1/search   - Return the VC policies

```
{  "policyMatch": {}
}
Returns
{ "policyTree": {} }
```

VC Rollout

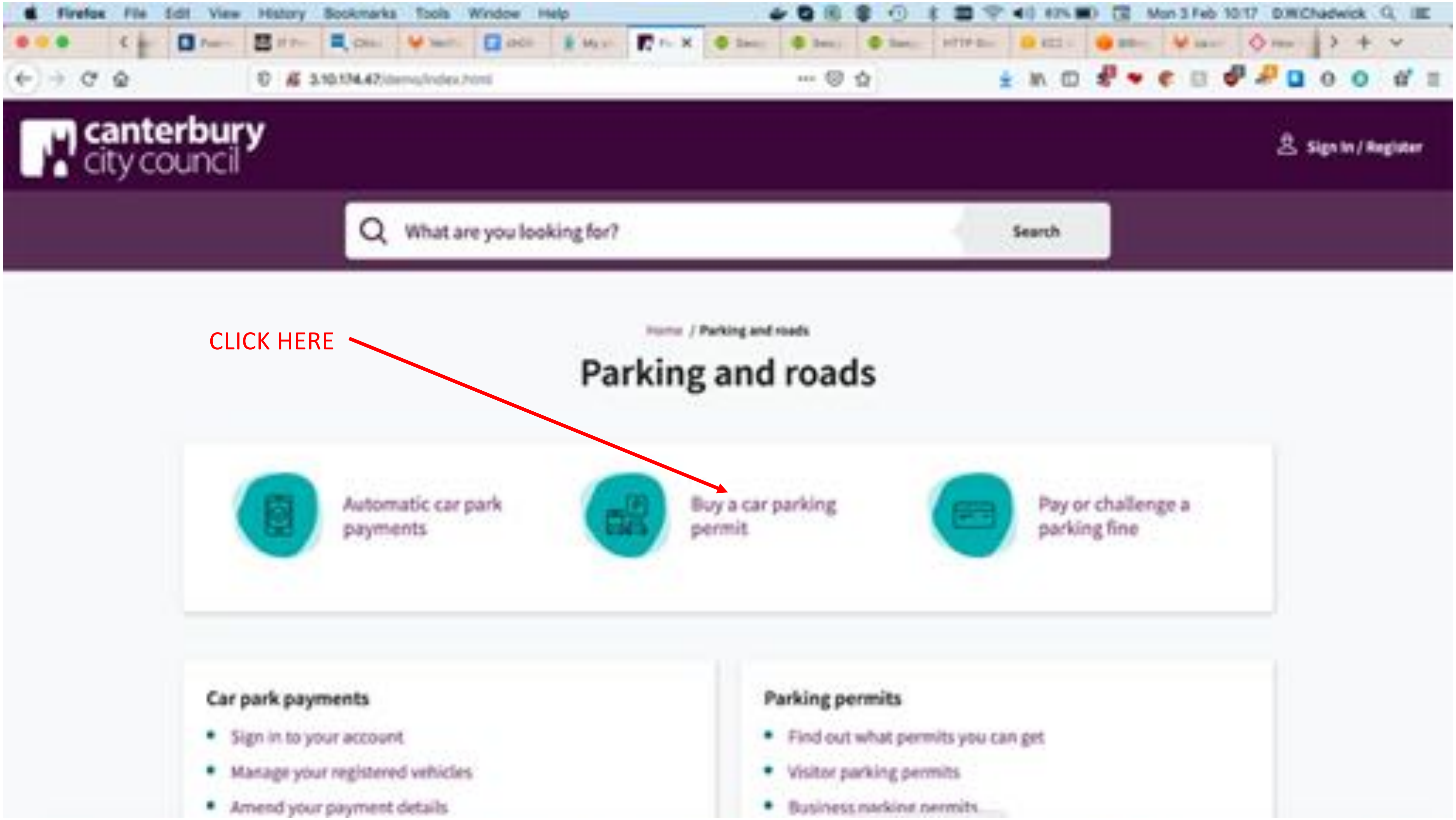
- Can start small where the SP and IdP are the same organization or community
- Choose an application that is currently not easy to implement online, or that is insecure, or too expensive E.g.
  - Making a doctor’s appointment or ordering a repeat prescription online. Patients are given a VC on their mobile phone when they visit the doctor, and thereafter they can go online, make the transaction and send their VC as proof of being a patient
  - Add a VC infrastructure to medical implants to ensure fine grained access control so that only doctors can manage the implants and patients can read them
  - Add to Fintech products to remove un/pws and increase the security

PSD2 - Revised Payment Service Directive

- FIDO2 VC model fits well with PSD2
- PSD2 requires 2 factor authentication
  - Something you have – mobile phone
  - Something you know – PW to access phone OR
  - Something you are – fingerprint to access phone
- PSD2 requires a dynamic link between the user and his paying account
  - Use of short lived VC requires phone to get a new VC from AA each time
- Payment Initiation Service Providers (PISPs) are ideal candidates to issue VCs to users

Compliance with GDPR

- W3c VCs make 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



CLICK HERE

Home / Parking and roads

Parking and roads

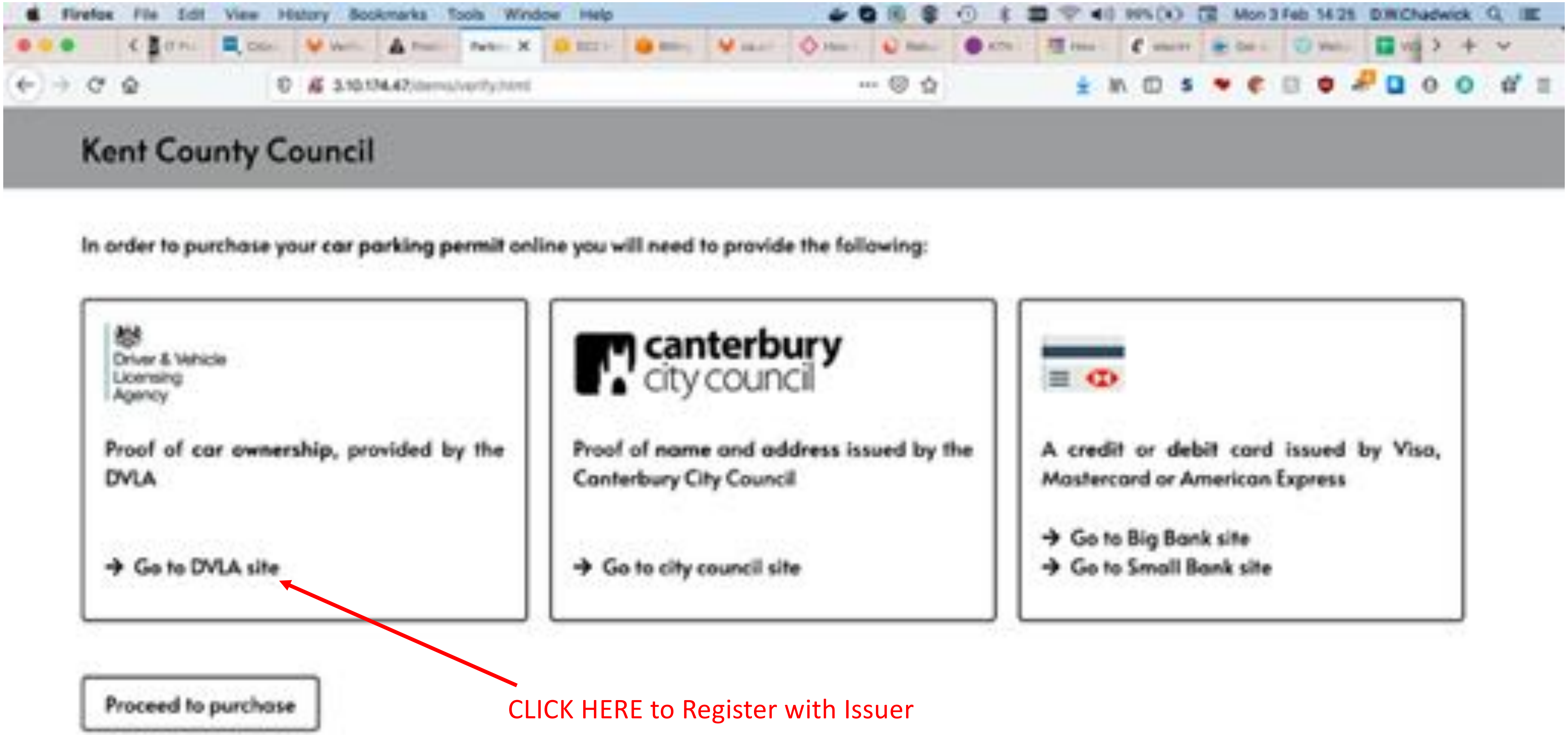
- Automatic car park payments
- Buy a car parking permit
- Pay or challenge a parking fine

Car park payments

- Sign in to your account
- Manage your registered vehicles
- Amend your payment details

Parking permits

- Find out what permits you can get
- Visitor parking permits
- Business parking permits



Firefox File Edit View History Bookmarks Tools Window Help
Mon 3 Feb 14:25 D.W.Chadwick
3.10.174.47/demo/verify.html

Kent County Council

In order to purchase your car parking permit online you will need to provide the following:

Driver & Vehicle Licensing Agency

Proof of car ownership, provided by the DVLA

→ Go to DVLA site

Proof of name and address issued by the Canterbury City Council

→ Go to city council site

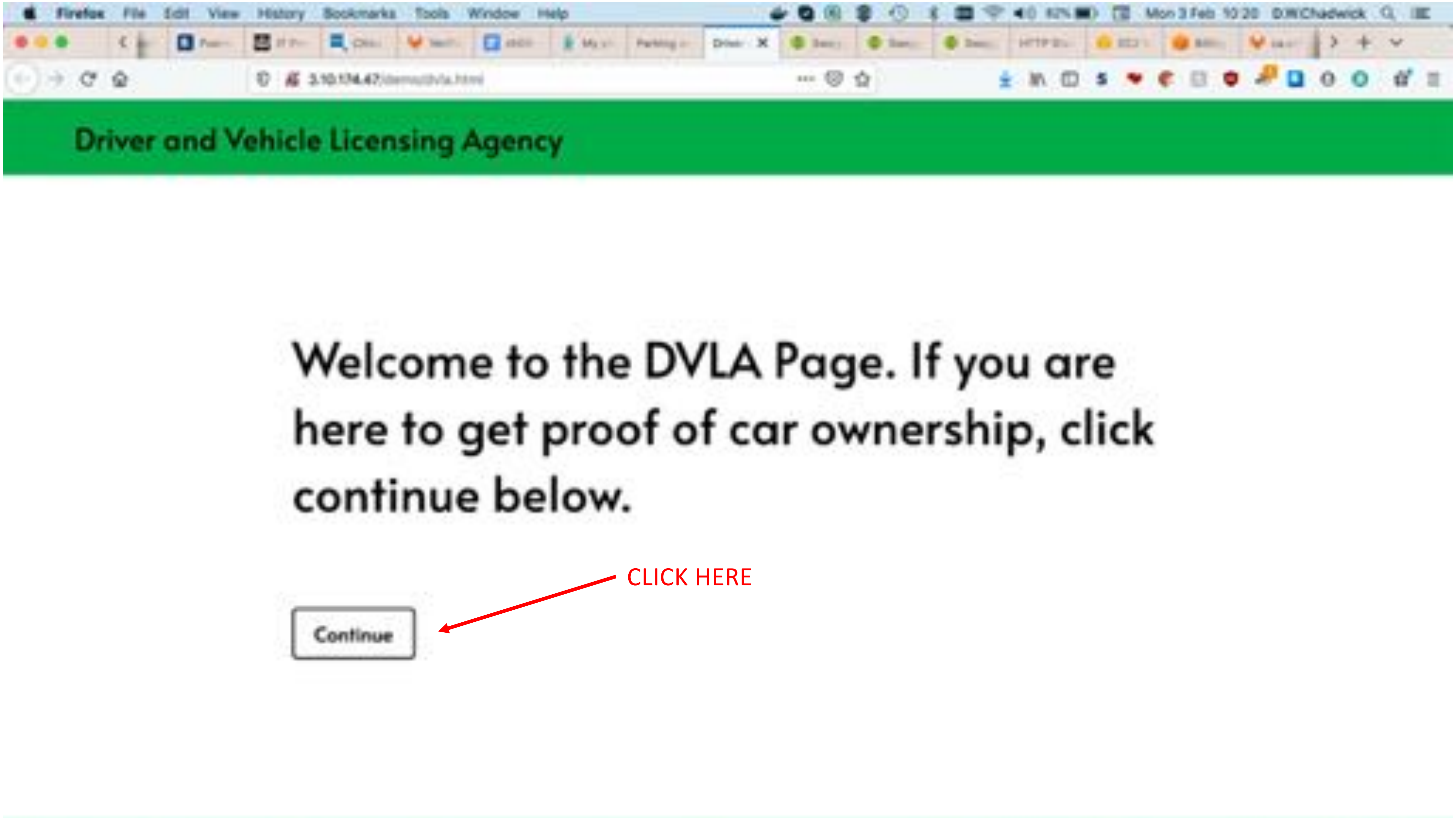
A credit or debit card issued by Visa, Mastercard or American Express

→ Go to Big Bank site
→ Go to Small Bank site

Proceed to purchase

CLICK HERE to Register with Issuer

Assuming the user has not already registered with the trusted issuers, then he/she must do this before performing the transaction


Firefox File Edit View History Bookmarks Tools Window Help
Mon 3 Feb 10:20 D.W.Chadwick
3.10.174.47/demo/dvla.html
Continue

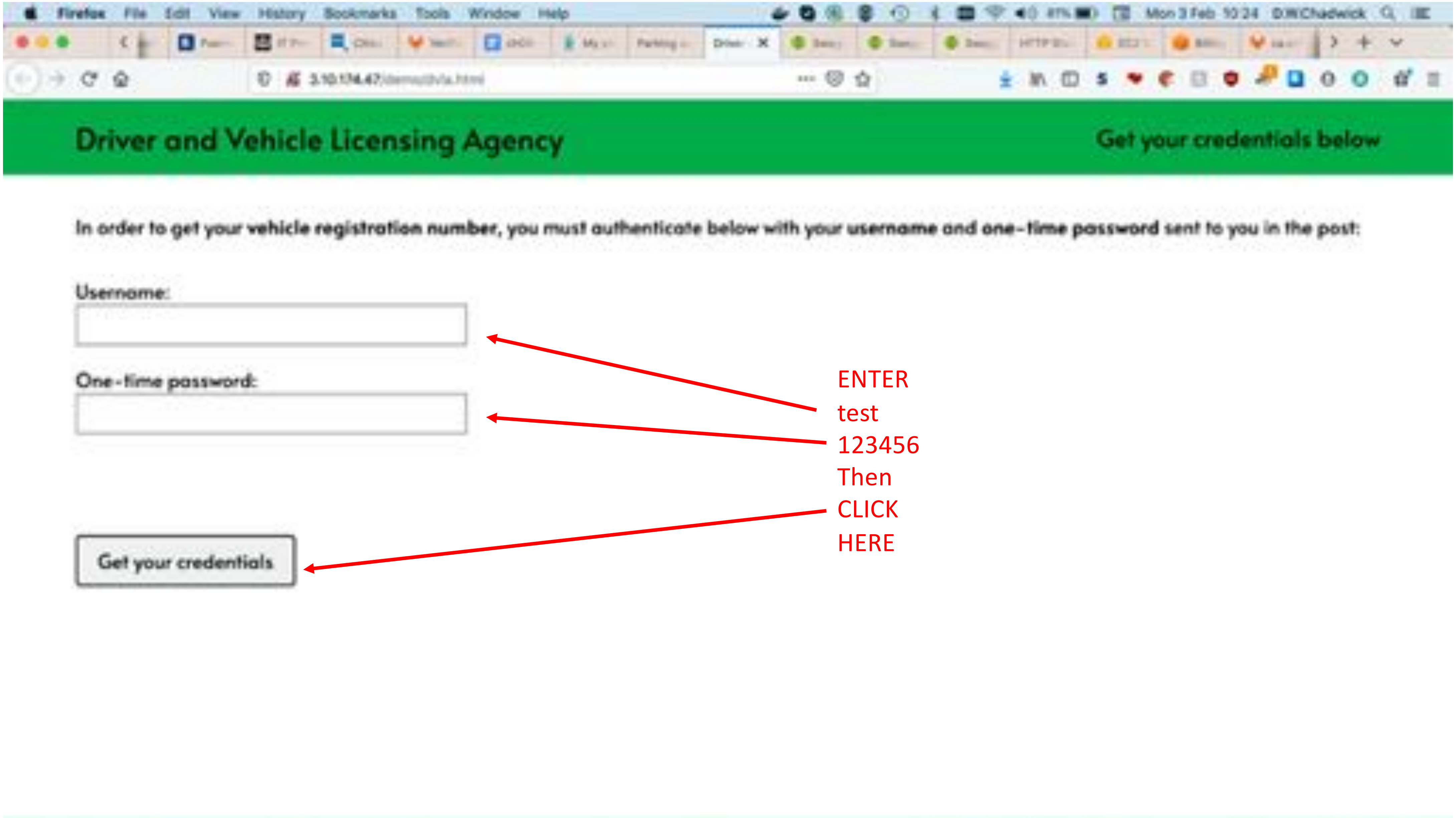
Driver and Vehicle Licensing Agency

Welcome to the DVLA Page. If you are here to get proof of car ownership, click continue below.

CLICK HERE

How the user registers with a VC Issuer is out of scope of the W3C standard, and VC Issuers may use any mechanism they deem appropriate, for example:
- send the user some one time credentials in the post
- ask them to visit a local office/branch of the issuer
- ask them to provide various government issued documents, etc.

Our implementation can cater for all of the above and more


Firefox File Edit View History Bookmarks Tools Window Help
Mon 3 Feb 10:24 D.W.Chadwick
3.10.174.47/demo/dvla.html

Driver and Vehicle Licensing Agency

Get your credentials below

In order to get your **vehicle registration number**, you must authenticate below with your **username** and **one-time password** sent to you in the post:

Username:

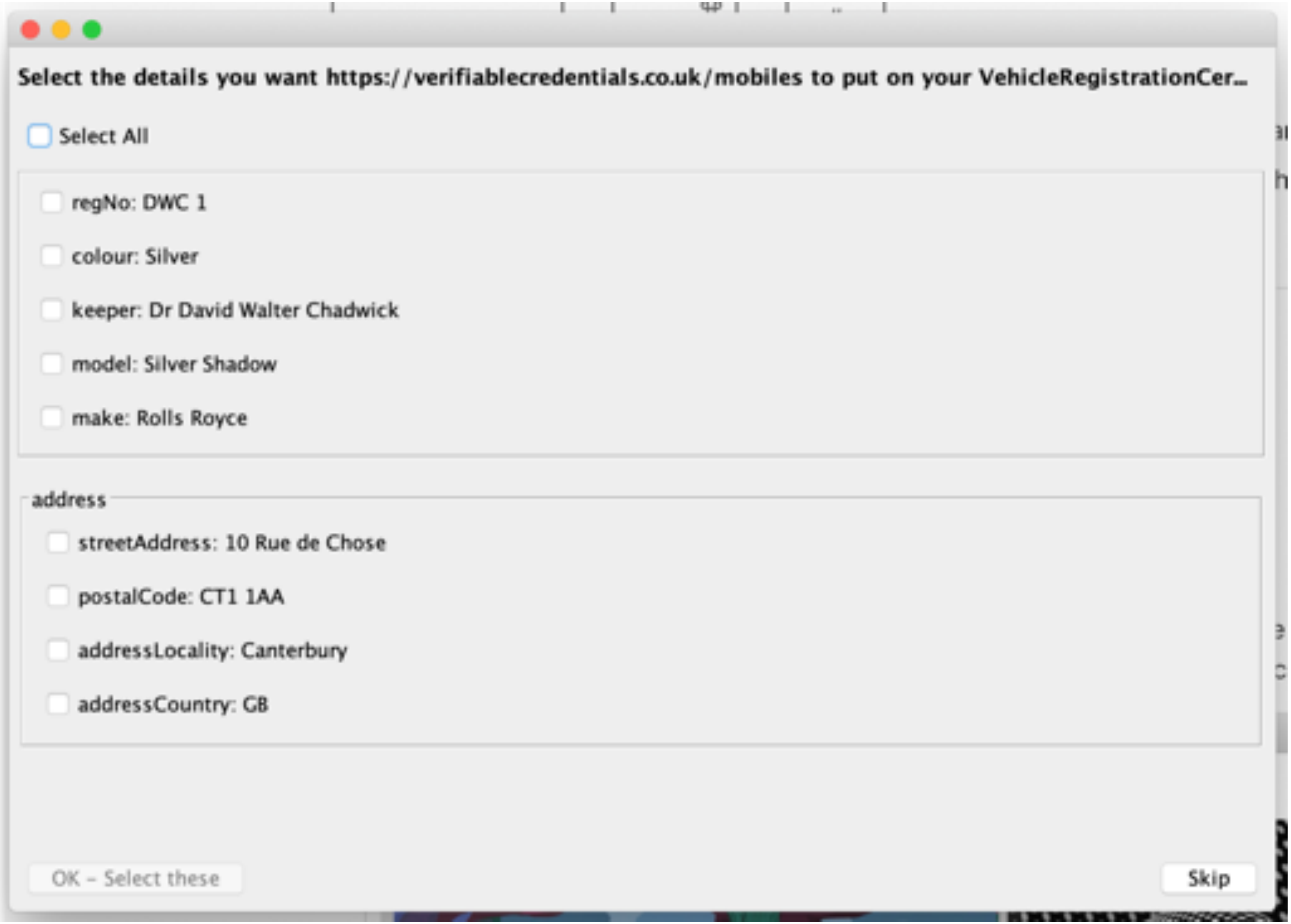
One-time password:

Get your credentials

ENTER
test
123456
Then
CLICK
HERE

User Consent

In Non-Automatic Mode, the User is asked to select which attributes may appear in the VCs the Issuer will subsequently issue



Select the details you want https://verifiablecredentials.co.uk/mobiles to put on your VehicleRegistrationCer...

□ Select All

□ regNo: DWC 1

□ colour: Silver

□ keeper: Dr David Walter Chadwick

□ model: Silver Shadow

□ make: Rolls Royce

address

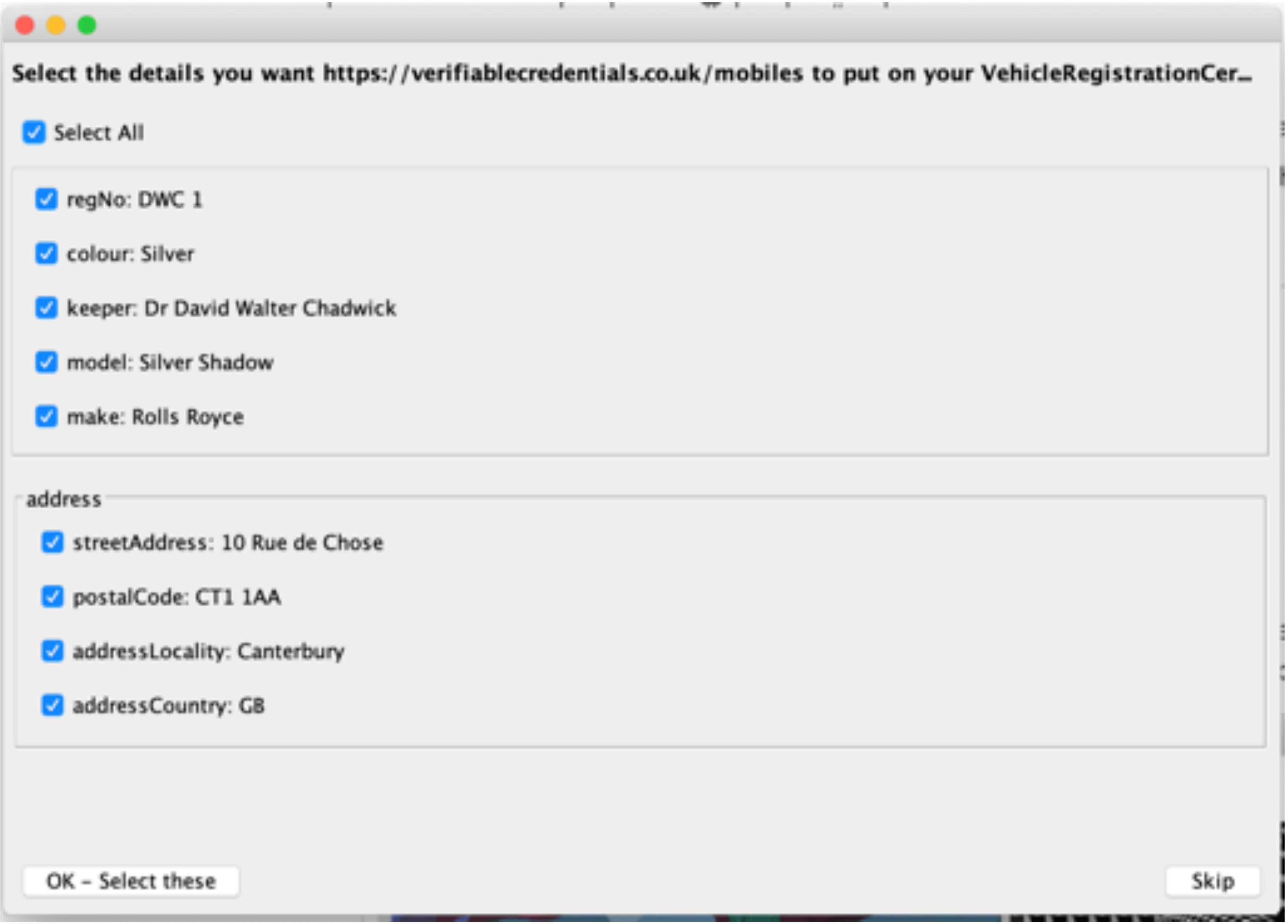
□ streetAddress: 10 Rue de Chose

□ postalCode: CT1 1AA

□ addressLocality: Canterbury

□ addressCountry: GB

The User can consent to All



Select the details you want https://verifiablecredentials.co.uk/mobiles to put on your VehicleRegistrationCer...

☑ Select All

☑ regNo: DWC 1

☑ colour: Silver

☑ keeper: Dr David Walter Chadwick

☑ model: Silver Shadow

☑ make: Rolls Royce

address

☑ streetAddress: 10 Rue de Chose

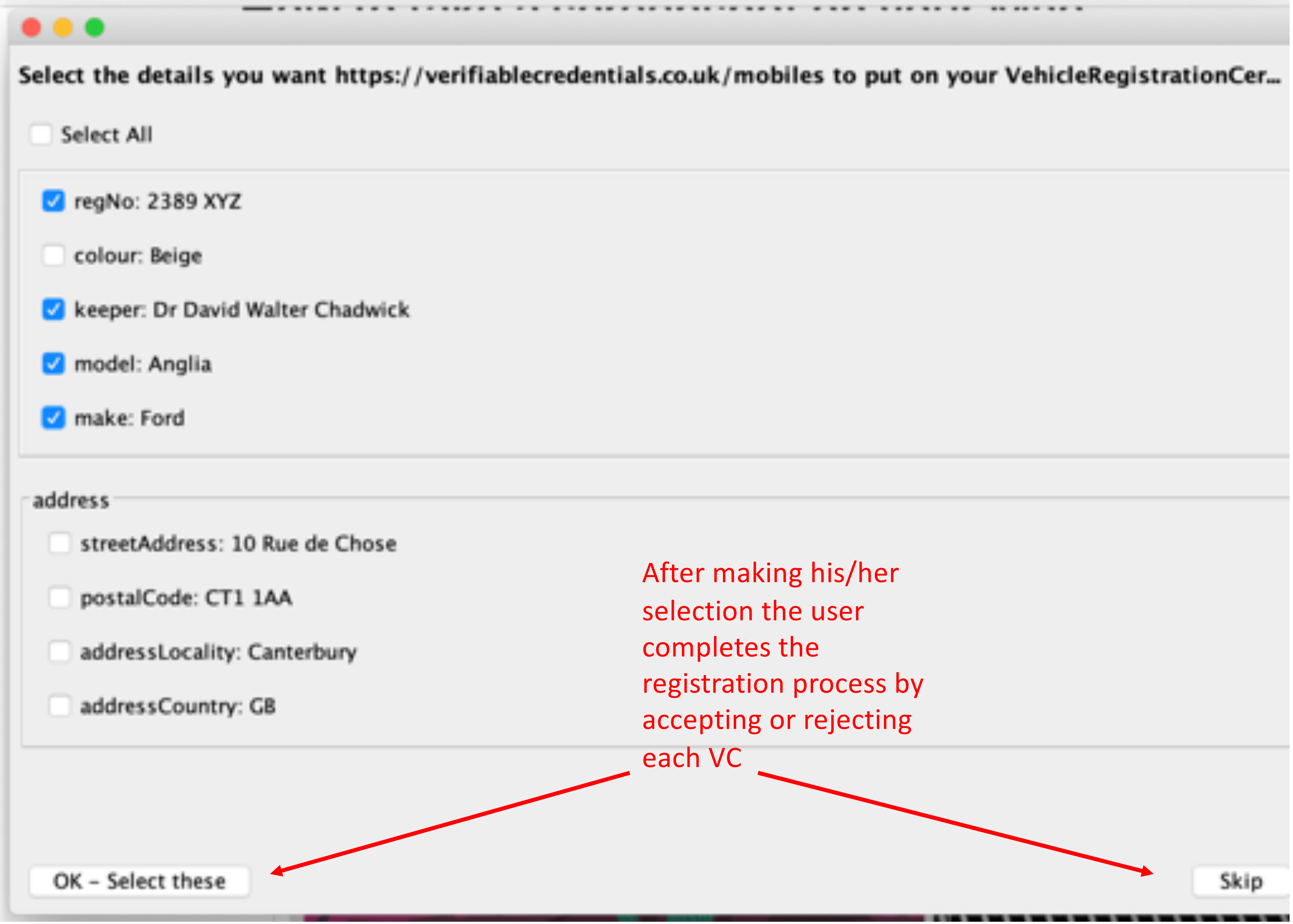
☑ postalCode: CT1 1AA

☑ addressLocality: Canterbury

☑ addressCountry: GB

Or a subset,

and may have multiple potential VCs to choose from



Select the details you want https://verifiablecredentials.co.uk/mobiles to put on your VehicleRegistrationCer...

☐ Select All

☑ regNo: 2389 XYZ

☐ colour: Beige

☑ keeper: Dr David Walter Chadwick

☑ model: Anglia

☑ make: Ford

address

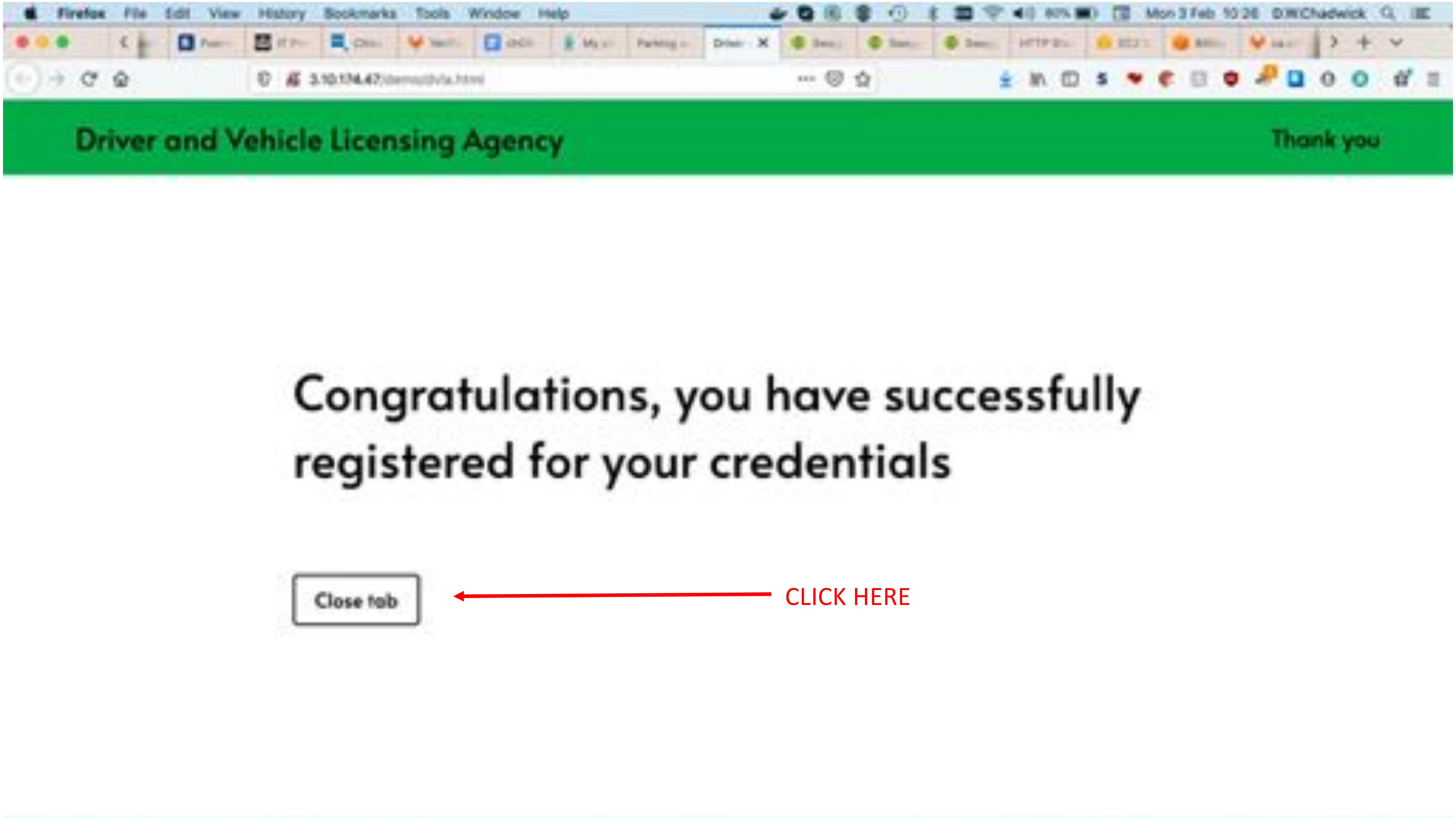
☐ streetAddress: 10 Rue de Chose

☐ postalCode: CT1 1AA

☐ addressLocality: Canterbury

☐ addressCountry: GB

After making his/her selection the user completes the registration process by accepting or rejecting each VC



Firefox File Edit View History Bookmarks Tools Window Help
Mon 3 Feb 10:26 D.W.Chadwick
3.10.174.47/demo/dvla.html

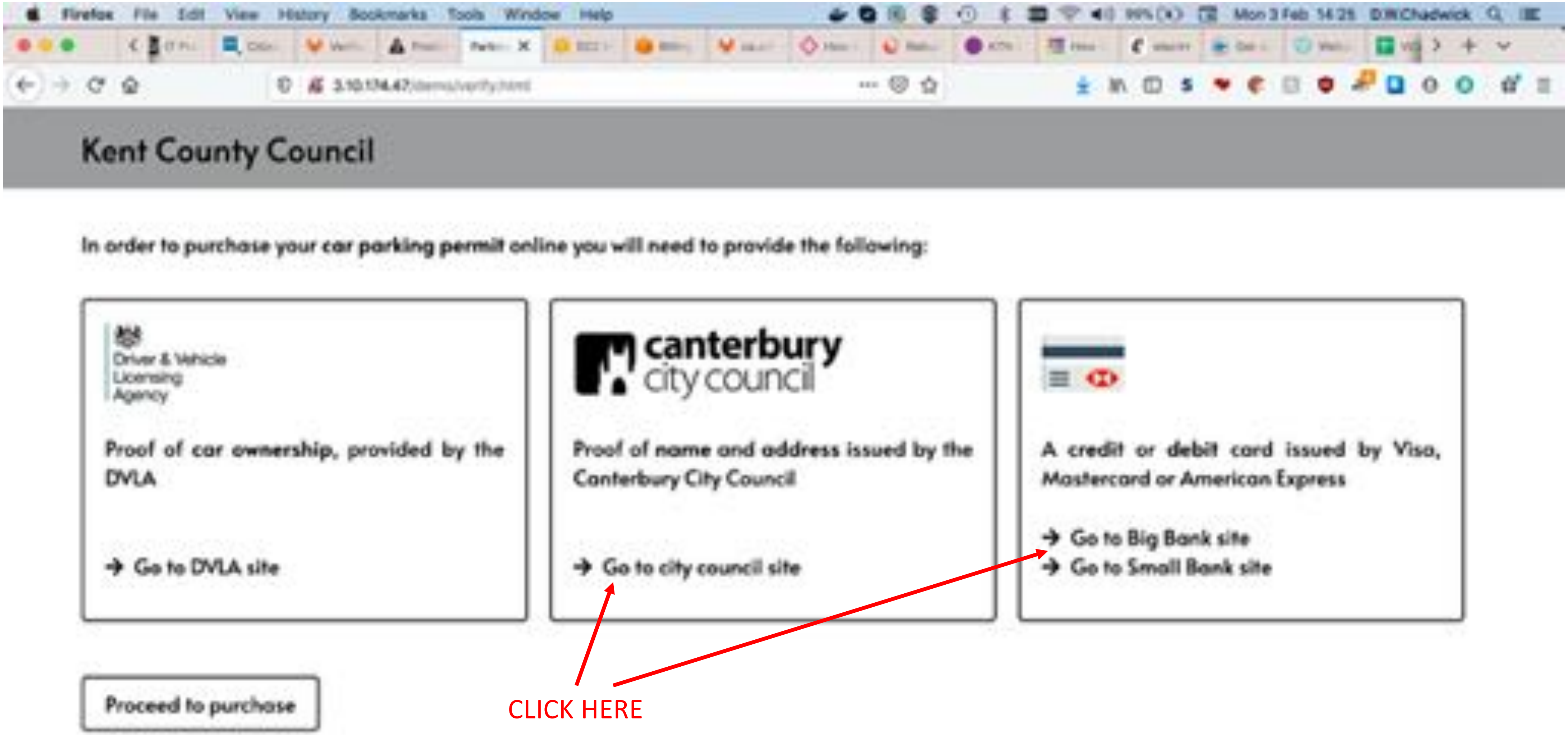
Driver and Vehicle Licensing Agency

Thank you

Congratulations, you have successfully registered for your credentials

Close tab

CLICK HERE



Firefox File Edit View History Bookmarks Tools Window Help
Mon 3 Feb 14:25 D.W.Chadwick
3.10.174.47/demo/verify.html
Driver & Vehicle Licensing Agency
canterbury city council

Kent County Council

In order to purchase your car parking permit online you will need to provide the following:

Proof of car ownership, provided by the DVLA

→ Go to DVLA site

Proof of name and address issued by the Canterbury City Council

→ Go to city council site

A credit or debit card issued by Visa, Mastercard or American Express

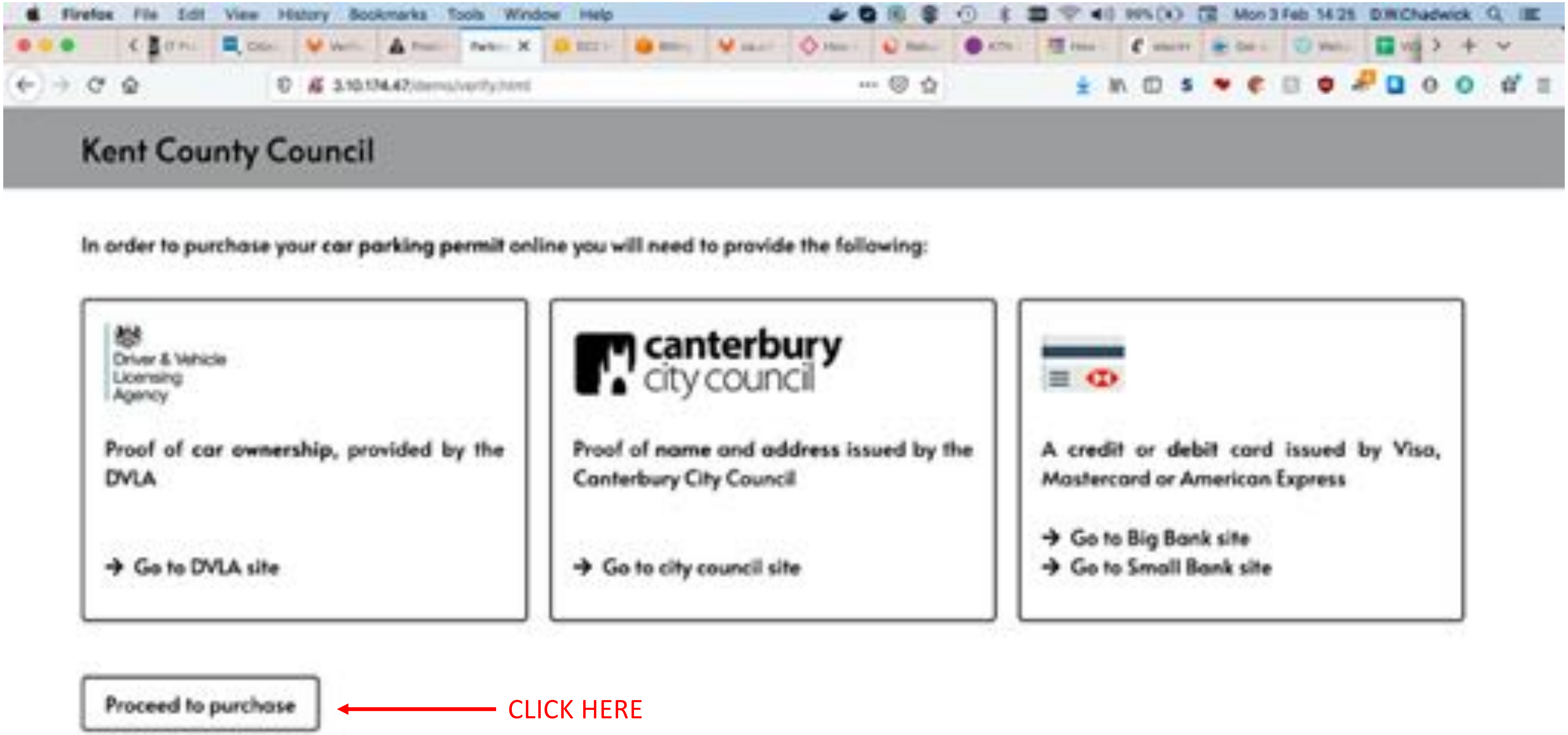
→ Go to Big Bank site

→ Go to Small Bank site

Proceed to purchase

CLICK HERE

Once the user has registered at the 3 VC issuers then he/she is ready to proceed with the purchase



Kent County Council

In order to purchase your car parking permit online you will need to provide the following:

Proof of car ownership, provided by the DVLA

→ Go to DVLA site

Proof of name and address issued by the Canterbury City Council

→ Go to city council site

A credit or debit card issued by Visa, Mastercard or American Express

→ Go to Big Bank site

→ Go to Small Bank site

Proceed to purchase

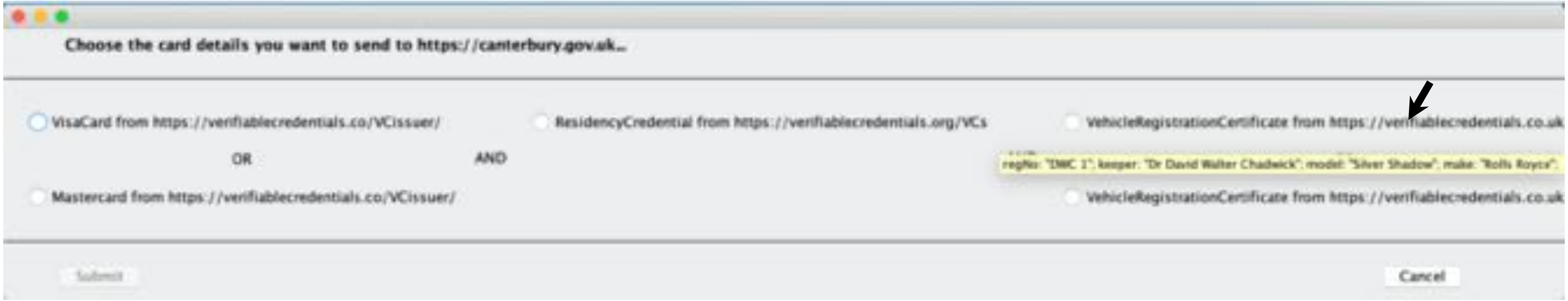
CLICK HERE

What happens now?

- In the background, the VC Holder app that is running on the user’s device picks up the policy of Kent County Council (the verifier). This says which VCs from which trusted VC Issuers are needed to purchase a car parking permit.
- The app checks to see if the user has already registered with the trusted VC issuers, and if they have, then
  - in automatic mode, it connects to each VC Issuer in turn and requests the required VC(s) to be issued
  - In non-automatic mode the app asks the user to choose between the alternative VCs that are available to him/her (e.g. visa or mastercard credit card)
- Selective Disclosure is automatic, since the verifier only asks for the VCs to contain the information that is required for the transaction
- If the user has not registered with sufficient trusted VC Issuers, then the user will be asked to register with them before proceeding, or
- If the user has registered with sufficient trusted VCs but did not consent to sufficient attributes being released, then the user will be asked to re-register with one or more VC Issuers

In non-automatic mode, the User is Presented with the Sets of VCs to choose from.

Placing the cursor on a VC reveals the attributes the SP has requested



Choose the card details you want to send to https://canterbury.gov.uk...

○ VisaCard from https://verifiablecredentials.co/VCissuer/

OR

○ Mastercard from https://verifiablecredentials.co/VCissuer/

AND

○ ResidencyCredential from https://verifiablecredentials.org/VCs

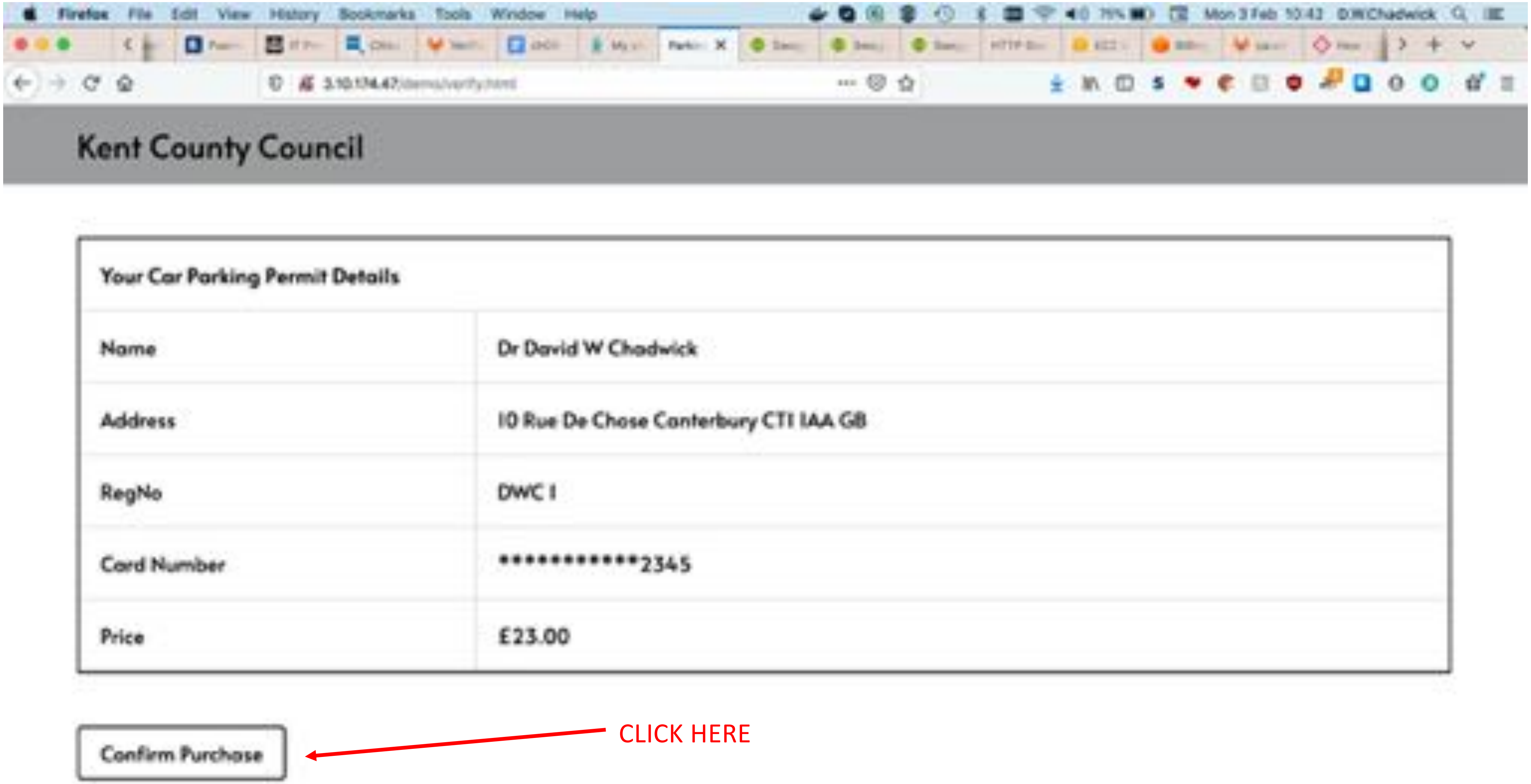
○ VehicleRegistrationCertificate from https://verifiablecredentials.co.uk

regNo: "DWC 1", keeper: "Dr David Walter Chadwick", model: "Silver Shadow", make: "Rolls Royce",

○ VehicleRegistrationCertificate from https://verifiablecredentials.co.uk

What happens next?

- Once the app has collected the required VCs, it creates a Verifiable Presentation (VP) containing the 3 VCs and signs them with the user's private key (especially created for this transaction)
- The app sends the VP to the verifier, which checks that it contains the 3 VCs required to purchase the car parking permit, and that all these VC belong to the owner of the private key that signed the VP
- Assuming all is OK, the verifier extracts the necessary information from the 3 VCs and displays them back to the user to confirm the purchase

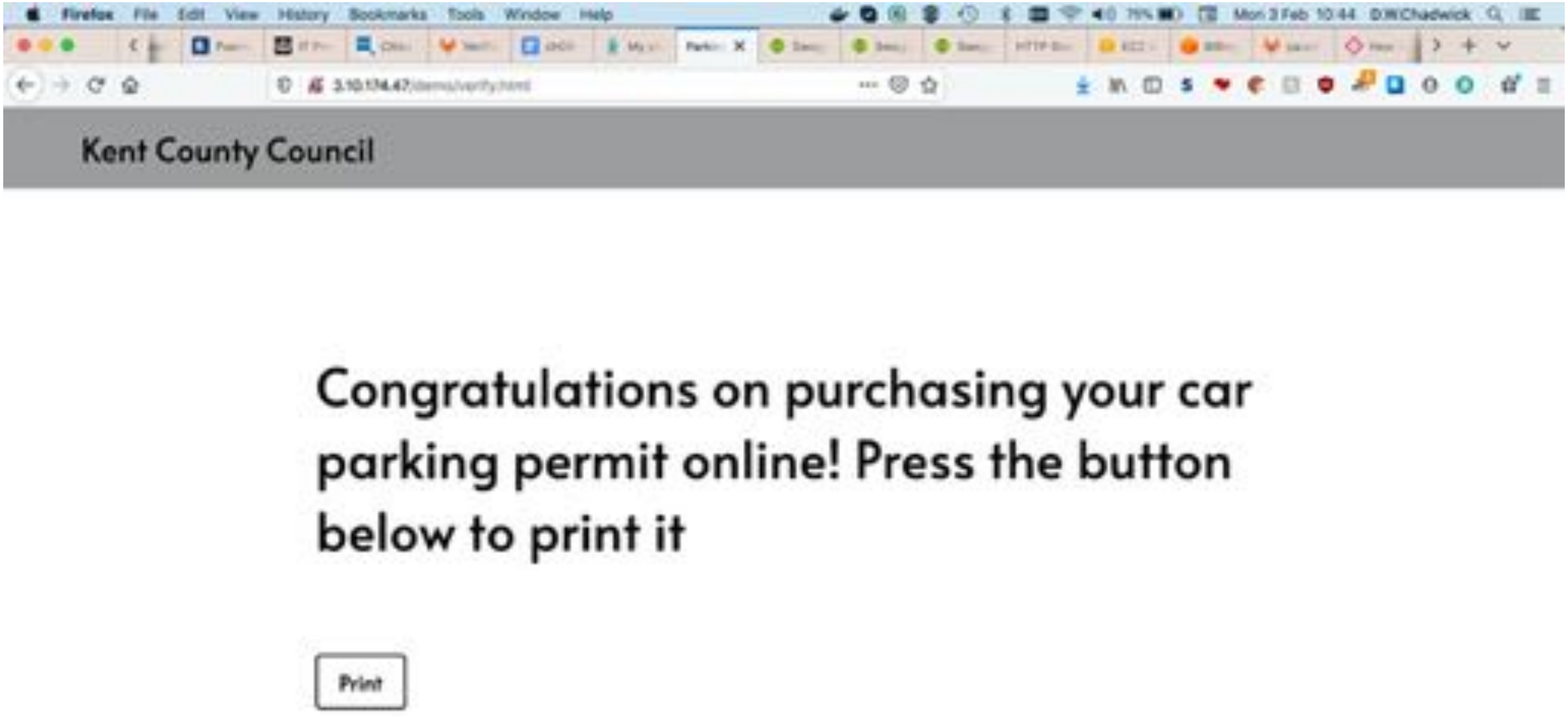

Firefox File Edit View History Bookmarks Tools Window Help
Mon 3 Feb 10:43 D.W.Chadwick
3.10.174.47/demo/verify.html

Kent County Council

Your Car Parking Permit Details	
Name	Dr David W Chadwick
Address	10 Rue De Chose Canterbury CT1 1AA GB
RegNo	DWC 1
Card Number	************2345
Price	£23.00

Confirm Purchase

CLICK HERE


Firefox File Edit View History Bookmarks Tools Window Help
71%
Mon 3 Feb 10:44 D.W.Chadwick
HTTP
3.10.174.47/demo/verify.html

Kent County Council

Congratulations on purchasing your car parking permit online! Press the button below to print it

Any questions?