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
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.

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

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

© 2019 University of Kent BCS meeting, University of Kent
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].

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

Issuer

Issuer’s Agent

Holder's Agent

Verifier

Wallet

Stores / Retrieves Credentials

Trusts

Issues Credential

Presents Credentials

Register Identifier(s), Keys, and Schemas

Verify Identifier(s) and Schemas

Verifiable Data Registry

© 2019 University of Kent

BCS meeting, University of Kent
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
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

User’s Browser

FIDO Client

Authenticator Specific Module API

FIDO Authenticator

Attestation Key

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

Certify Compliance

FIDO Metadata Service

Service Provider

Web Site

FIDO Server

Public Key DB

Public Key/Attribute DB

FIDO Authz Module

FIDO Ready Smart Device

SOP

Authn Keys

© 2019 University of Kent

BCS meeting, University of Kent
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


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.
Registration Step 3. NHS asks user which credentials he wants. User chooses and NHS remembers (in this case there is no choice)
Registration Step 4. NHS confirms recording of credential
Registration Step 5. The user goes to the hospital consultant and registers to use the consultant’s service.
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.
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)
Registration Step 8. Hospital confirms recording of credential

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.
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)
Use Step 4. Hospital Patient Menu is displayed. User chooses Consultancy
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)
Use Step 6. User confirms selection with fingerprint

Login Confirmation

Please use your fingerprint to confirm login.

CANCEL
Use Step 7. Consultancy Menu is Displayed
Use Step 8. Book Appointment

Select your desired date and time of day:

**AM, 03/09/2017**

Select a free slot:

Book
Use Step 9. Confirmation Message

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

Select one or more appointments to cancel:

- 10:30, 9/3/117

Cancel Appointment(s)
Use Step 11. Order Repeat Prescription

Repeat Prescription

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?