So you want to use Digital Credentials?

You're now facing a myriad of choices!

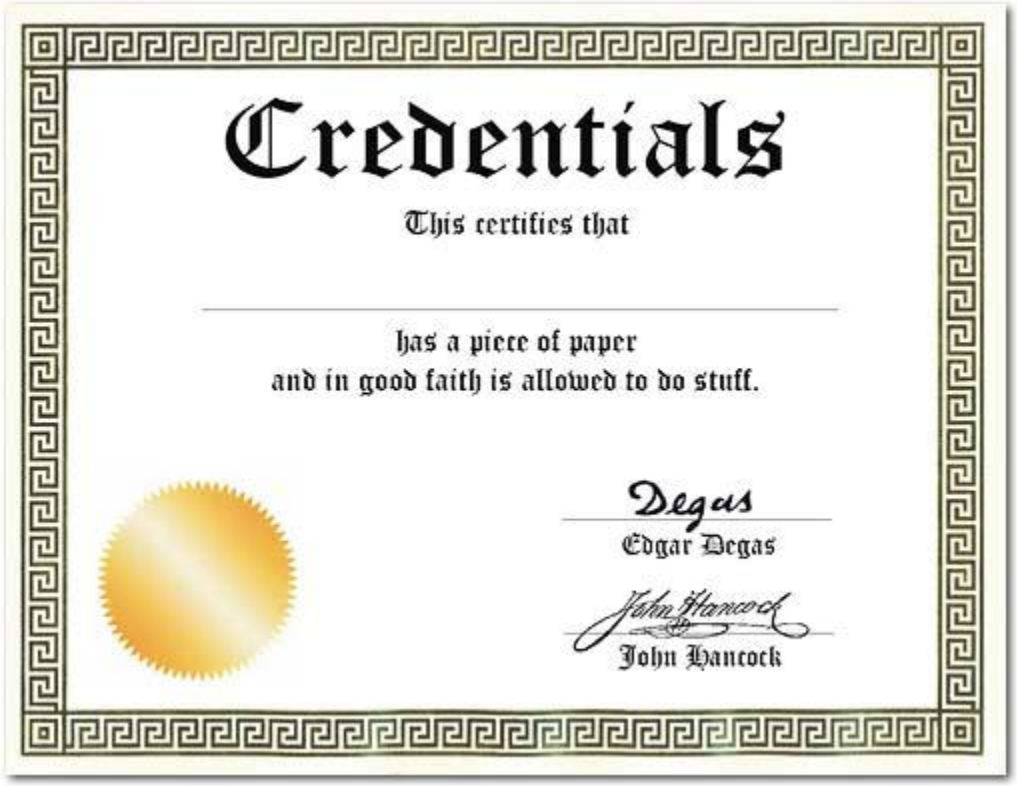
Dr. Michael B. Jones

Principal, Self-Issued Consulting

#EIC2025

The Promise of Digital Credentials

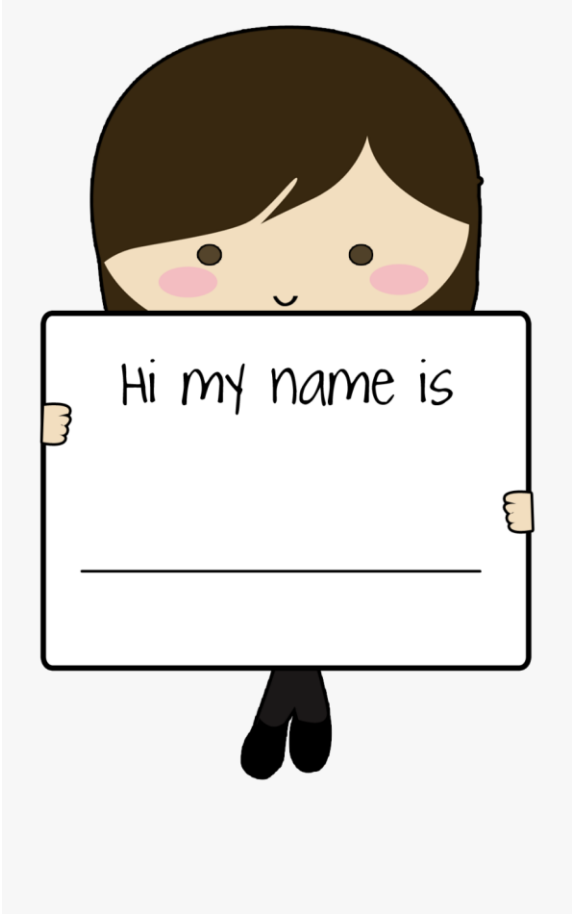
- An identity innovation facilitating user control and choice
- You decide when and where to use credentials you control
- Like your physical driver's license or ID card, the issuer doesn't know where you've used it
- Unlike your physical driver's license or ID card, you can reveal only the subset of information you choose to the recipient



The myriad of choices you’re now facing…

What are they called?

- For starters, we don’t even agree on what to call them!
- Do you call them?
  - Digital Credentials
  - Verifiable Credentials
  - Verifiable Digital Credentials
  - Credentials
  - Tokens
  - Assertions
  - Certificates
  - …
- Take your pick!



What kind(s) of digital credentials to use?

W3C Verifiable Credentials

- The original
- JSON-based credentials using JSON-LD
  - As Markus said yesterday, developers tend to get `@context` values wrong
- Three variants: VC Data Model 1.0, 1.1, and 2.0
  - 2.0 not compatible with 1.0 and 1.1 but arguably an improvement
- Two classes of signing methods
  - VC-JOSE-COSE – Signs using IETF-defined signing mechanisms
  - VC-DATA-INTEGRITY – Custom representation signing over N-Quads or canonicalized JSON
- A myriad of choices just within this credential format!

ISO mDOC

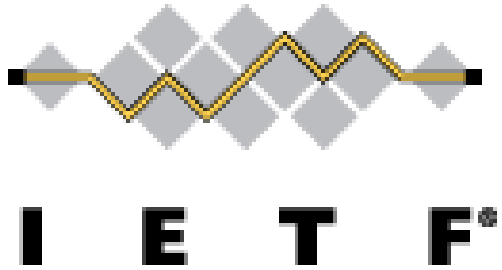
- CBOR-based credential format
- Supports salted hash-based selective disclosure of claims
- mDOC is base structure other credential formats based on
  - In particular, mDLs (Mobile Driving License)
- Claims have a namespace component
  - mDL namespace is `org.iso.18013.5.1.mDL`
- Claim names defined within mDL namespace
  - `family_name`
  - `portrait`
  - `age_over_`*NN*

ISO mDOC

- mDOCs also used for credentials other than mDLs

- Personal Identifier Documents (PIDs)
  - EU PID namespace is `eu.europa.ec.eudi.pid.1`
  - German PID namespace is `eu.europa.ec.eudi.pid.de.1`
- Health Certificates
  - Mobile International Certificate of Vaccination (micov) namespace is `org.micov.medical.1`

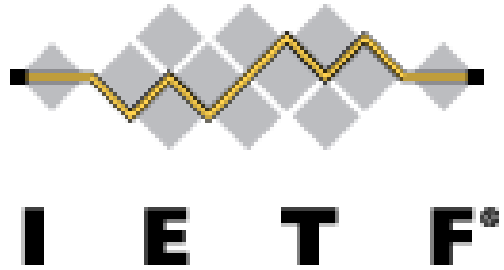
Selective Disclosure JWT (SD-JWT)



- JSON-based credential format
- Supports salted hash-based selective disclosure of claims
- Claims not namespaced
- Claims from IANA JWT Claims Registry
  - `family_name`, etc.

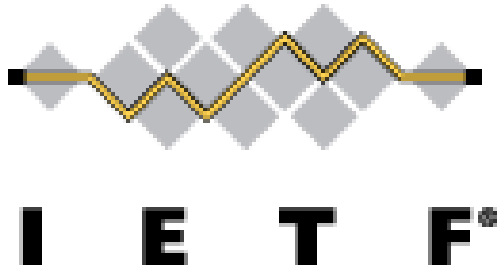
- SD-JWT VC based on SD-JWT
  - Adds validation and processing rules
- Both in development in the IETF OAuth working group

Selective Disclosure CWT (SD-CWT)



- CBOR-based credential format
- Supports salted hash-based selective disclosure of claims
- Claims not namespaced
- Claims from IANA CWT Claims Registry
  - Claim identifiers are small binary integers, rather than strings
- In development in the IETF SPICE working group

JSON Web Proof (JWP)



- Credential format supporting zero-knowledge proofs
  - For instance, enables proof of age-over-21 derived from birthdate without disclosing birthdate
- BBS signatures one proof mechanism supported
  - In development in the IRTF CFRG working group
- Two serializations – JSON and CBOR
  - JSON claims from IANA JWT Claims Registry
  - CBOR claims from IANA CWT Claims Registry
- In development in the IETF JOSE working group

X.509 Certificate

- ASN.1-based certificate format
- Does not support selective disclosure of attributes
- Attribute names are Object IDentifiers (OIDs)
  - Subject Alternative Name OID is `2.5.29.17`
  - Birth Family Name OID is `2.23.42.2.3`

- Many different certificate profiles
  - TLS certificates
  - Covid Vaccination certificates

How to communicate them?

Issuance and Presentation

- Credential Issuance
  - An issuer communicating a digital credential to the person’s wallet
- Credential Presentation
  - A wallet presenting a digital credential to a verifier
  - May involve selective disclosure or zero-knowledge proofs

- Multiple mechanisms to do each

Credential Issuance Mechanisms

- Bespoke issuance mechanisms common
  - For instance, custom mechanisms for adding mDLs to Apple, Google wallets
- Some are credential-format specific
  - What might work for mDLs might not work for SD-JWTs

- OpenID for Verifiable Credential Issuance
  - Credential format independent issuance protocol

Credential Presentation Mechanisms

- Two kinds of presentation mechanisms
  - In-person presentation
  - Remote (Internet) presentation
- In-person presentation uses proximate communication
  - Near-Field Communication (NFC)
  - Bluetooth Low Energy (BLE)
- Remote presentation uses Internet communication or APIs
  - OpenID for Verifiable Presentation
    - Credential format independent presentation protocol
    - Both OAuth-based protocol and browser API defined
  - 18013-7 Annex C is AustRoads mechanism
    - mDOC specific

More Credential Communication Options

- W3C Digital Credentials API (DC API)
  - Uses OpenID4VP
- W3C Verifiable Credentials API (VC API)
  - *(no, they're not the same!)*
- DIDComm

How do you choose credentials?

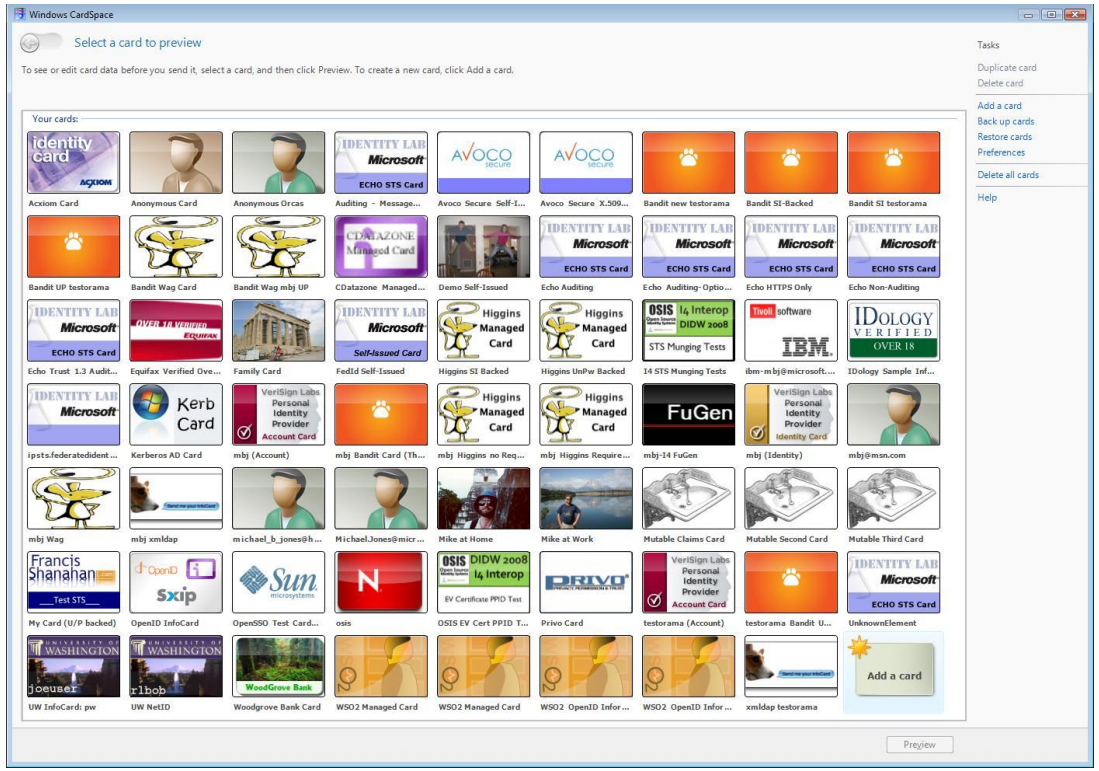
Query Languages

- Multiple query languages for selecting credentials in use
  - Presentation Exchange (PE)
  - Digital Credential Query Language (DCQL)

Credential Choice User Interfaces

- Wallets implement user experiences for choosing credentials
- Platforms implement user experiences for choosing wallets

- *Best practices and usability a work in progress!*



Establishing Trust

Deciding whether to interact with a party (or not)

Multiple Different Ways to Establish Trust

- Trusted Lists of Participants
  - Simple – doesn't scale
- X.509 Certificates and Certificate Chains
  - Requires custom certificate issuance & update mechanisms
  - Requires maintaining list of trusted certificate authorities
- Federations
  - Trust a party when you and they share a common trust anchor
  - OpenID Federation model
  - Scalable

Thought Experiment on Trust Establishment

- Let’s assume the EU digital wallet projects wildly succeed
- People in Portugal will have become accustomed to using their credentials in Spain and Germany and Greece and Estonia
- But then they’ll want to use their credentials in exotic places like Canada and Singapore and Kenya and the UK
- How will we make that happen?

Usability is Everything

Will people be able to use it *and want to*?

- InfoCards enabled
  - Wallet with credentials you choose when and where to use
  - Passwordless login
  - *Sound familiar? ;-)*
- InfoCard usability a cautionary tale
  - *Most people had no idea how to use them or why they would want to*
  - The few who succeeded asked "How could I have logged in? – I didn't type a password"
- Usability lessons still apply today

Building Ecosystems is Hard

Must be compelling value for all parties

- Building ecosystems requires all necessary parties to voluntarily and incrementally adopt system
- They will only adopt if there is value for them doing so ***now***
- Visions of how great things will be once everyone does it won't get the job done
- Getting from zero to ubiquitous is hard!

Katryna Dow on Building Ecosystems

- As global citizens, we are constantly crossing borders
- Borders are digital but identity is local
- Pillars of Ecosystem Success
  - Trust Frameworks
  - Open Standards
  - Governance Models
  - Public/Private Collaboration
  - User-Centric Design
- How do you build trust at scale?
  - Mutual Recognition
  - Shared Assurance Levels
  - Transparent Verification

Juliana Cafik on Digital Credentials

- Use digital credentials to solve unsolved real-world problems
  - For instance, reducing online fraud a worthy objective
- The Verifier is not the journey's end
  - Verified credential is an input to a business process
- Winning will take doing all the hard work to make it easy and safe
- The protocols and data formats are not the point
  - Solving real problems is the point

Standards are about making choices

- *The subject of my talk last year*
- Applies to digital credentials
- Interoperability requires that the same choices be made by interacting participants
  - No substitute for working together with others to make the right choices
- ***So make good ones together!***

Thank You!

The people behind wwWallet

This presentation available at
https://self-issued.info/

#EIC2025