Digital Credentials and Issuance Protocols

A joint effort by the global community of experts

Andrew Hughes, Dr. Torsten Lodderstedt

Andrew Hughes

Director of Identity Standards

Ping Identity

Dr. Torsten Lodderstedt

Managing Director

yes IDP GmbH

A story in four parts

Part 1: Setting the context
Part 2: Types + features of credentials
Part 3: Credential issuance protocols
Part 4: “Holder Binding”

Part 1: Setting the context

Andrew Hughes
Director of Identity Standards, Ping Identity

Digital Credentials

A digital credential conveys data that is an authentic representation of information held in a registry at the time of issuance.

The packaging, security features and metadata of a digital credential gives a credential recipient assurance and confidence that the digital credential is genuine

Digital credentials come in many shapes, types and formats.

Issuance Protocols

A digital wallet should be able to request, receive, validate and store digital credentials of many types and formats.

The means to obtain a digital credential and place it in a digital wallet must be standardized to enable any digital credential issuer to securely and efficiently interface with any digital wallet.

We call these means Digital Credential Issuance Protocols.

Credential Issuer and Wallet Requirements

Credential issuers have requirements that support their usage scenario. Some credentials are high value, requiring strong protection and assurance at all times. Some credentials require less protection.

Wallet software and hardware will have capabilities based on design approach, implementation choices and requirements as determined by the wallet development team.

Standardization Reduces Risk

Credential issuers may wish to require minimum wallet capabilities for their issued credentials.

Issuance protocol standardization is necessary to enable inter-operation and unlimited innovation for issuers and wallet developers.

Credential issuance protocols must accommodate these needs and more.

This Session

Work intensity to define issuance protocol requirements, specifications and standards has increased in recent years.

Each group has different stakeholders, different approaches, different priorities.

This session will give an overview of some emerging protocol specification work from several standardization organizations.

Part 2: Types + features of credentials

Dr. Torsten Lodderstedt
Managing Director, yes IDP GmbH

What

- As a community effort, we are creating a **Credential Profile Comparison Matrix**
  https://docs.google.com/spreadsheets/d/1X93ptJcmfX1NZEo5E7ElnqJ-knDS4Dj6JOYSJ_2PsUw
- It is accompanied by a **Guiding Paper** located at
  https://github.com/WebOfTrustInfo/rwot11-the-hague
- Summary Presentation
  https://www.linkedin.com/posts/idunion_credential-format-comparison-and-idunion-activity-7008024119598276609-0pS-/
- Paper is done, the matrix is work in progress, and probably continues to be

Why

- The different Credential Profiles have strong follower communities
- For many good and obvious reasons, they are convinced their stack is “favorable”
- Having a **fact-based comparison** is long overdue
- With this work, we **facilitate an objective discussion and comparison**
- This will ease technical and non-technical decision making

How

- A comparison matrix is created
- Comparison categories (6) and criteria (50) are derived
- Experts from the different stakeholder groups are engaged to obtain their input

Key milestones 2022/2023 so far

Kick-off IIWXXXIV	Task force work by Torsten, Paul, Andre				Paper RWOT11	Task force work	Experts IIWXXXV	Task force work				RWOT11 Final + IIWXXXVI
APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR

Matrix

Too large to easily display as slide - see here:

https://docs.google.com/spreadsheets/d/1X93ptJcmfX1NZEo5E7ElnqJ-knDS4Dj6JOYSJ_2PsUw

50 Criteria

Credential Profile	Credential Format	Signing Algorithm	Revocation Algorithm	Key Management	Trust Management
Formal Specification	Implementation Support (e.g. Libraries)	Implementation Support (e.g. Libraries) / Active Community	Implementation Support (e.g. Libraries) / Active Community	Implementation Support (e.g. Libraries) / Active Community	Implementation Support (e.g. Libraries) / Active Community
IPR Policy	IPR Policy	IPR Policy	IPR Policy	IPR Policy	IPR Policy
Implementations	Specification	Specification	Specification	Specification	Standardization (Body, Process)
	Standardization (Body, Process)	Standardization (Body, Process)	Standardization (Body, Process)	Infrastructure for Key Resolution	Specification
	Technology Readiness Level	Technology Readiness Level	Technology Readiness Level	Key Rotation	Description
	Encoding Scheme	Recognition by government authorities (NIST, BSI, ...)	Recognition by government authorities (NIST, BSI, ...)	Key History	
	Rich Schemas/Semantic	Performance	Category	Party	
	Crypto Agility	Hardware support	Performance		
	Selective Disclosure	Unlinkability/Uncorrelatability /Blind signatures possible	Observability		
	Predicates	Security strength	Traceability		
	Compatibility with Signing Algorithms	Post-quantum security	Scalability		
	Compatibility with Key Management Methods (Issuer)		Offline Friendliness		
3	**12**	**11**	**12**	**7**	**5**

Insights

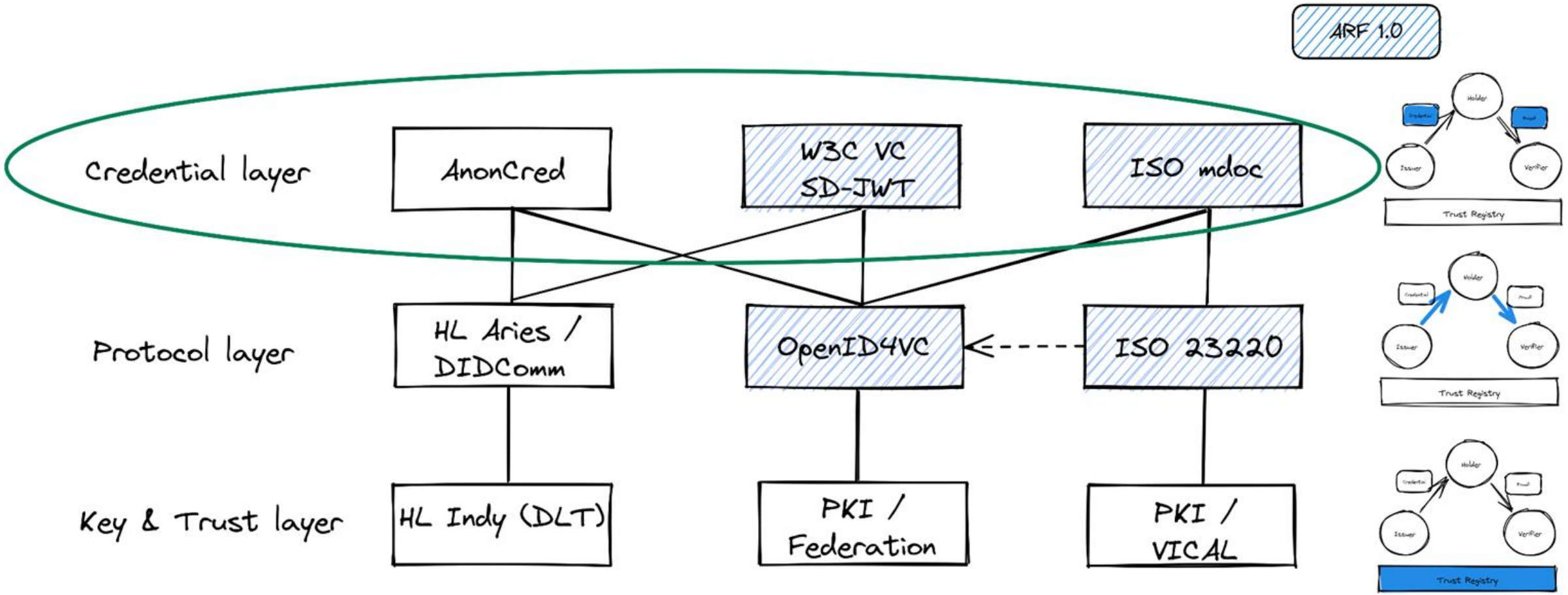
- The obvious: So many credential formats
- The number of profiles is even higher (by an order of magnitude) through combination with signature algorithm, key management, revocation, trust management
- A lot of clarity is achieved with the methodology
- Not all data items could be collected yet

Evaluation

[1] : BoundBBS+ offers unlinkability, BBS+ with did:key holder binding not
[2] : JSON-LD as pure data payload is possible
[3] : fast maturity increase expected

	Anoncreds	W3C JSON-LD /BBS+	W3C JSON-LD /EdDSA	W3C JWT-VC	W3C SD-JWT-VC	ISO mdoc
Selective Disclosure	yes	yes	no	no	yes	yes
Unlinkability	yes	yes[1]	no	no	no	no
Hardware security support	no	no	yes	yes	yes	yes
PQC & cryptographic agility	no	no	yes	yes	yes	yes
Standardisation	Community Specification	W3C Recommendations / IETF	W3C Recommendations / IETF	W3C Recommendations / IETF	W3C Recommendations / IETF	ISO 18013-5 / ISO23220-2
Technology Readiness Level	6-8	6-7	7-8	7-8	4-5[3]	8-9 (on-site) 5-6 (remote)
Predicates	yes	no	no	no	no	no
Semantic support	no	yes	yes	no[2]	no[2]	no

A layered Architecture



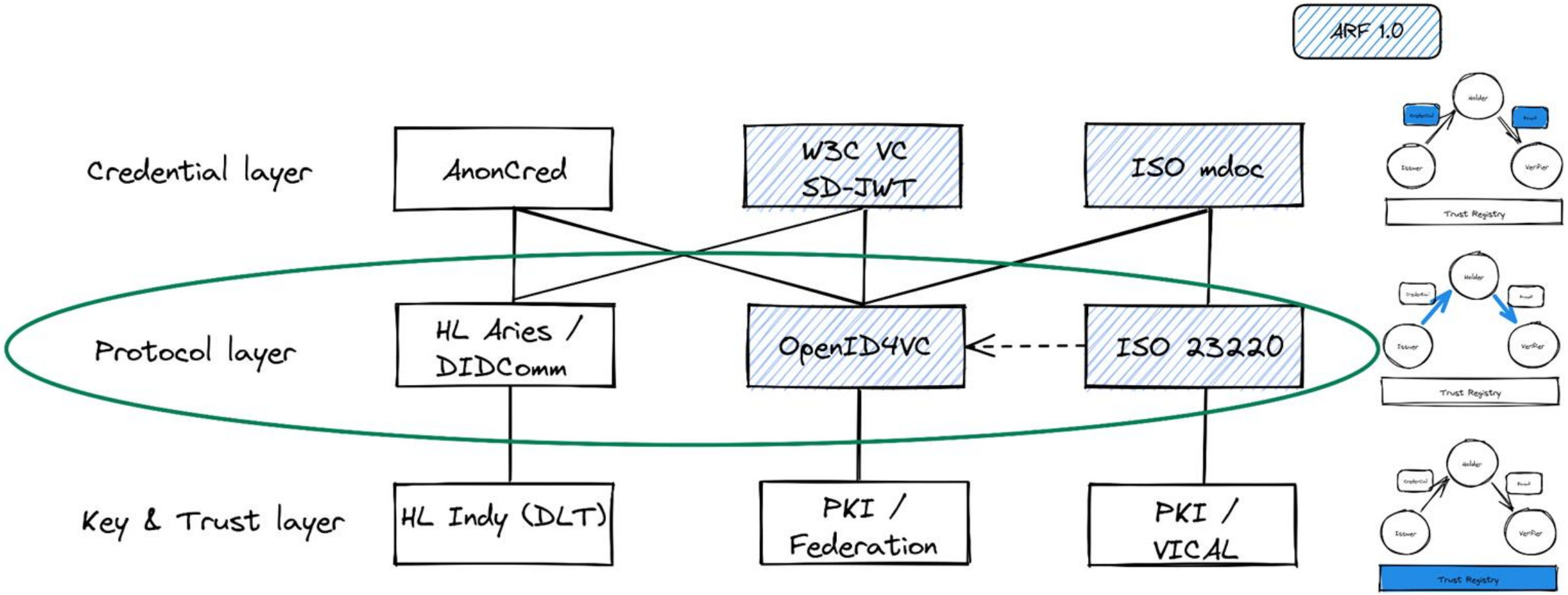
What's happening in 2023

ToDo	Who	When
Finalize and publish guideline paper	RWOT11 experts group	April 2023
Matrix expert discussion cont'd at IIWXXXVI Mountain View	All experts	April 2023
Presentation at EIC 2023 Berlin	Bastian, Lodderstedt, Kudra, Hughes (remote)	May 2023
Presentation at Identiverse 2023 Las Vegas	Hughes, Lodderstedt	June 2023

Part 3: Credential issuance protocols

Dr. Torsten Lodderstedt
Managing Director, yes IDP GmbH

A layered Architecture

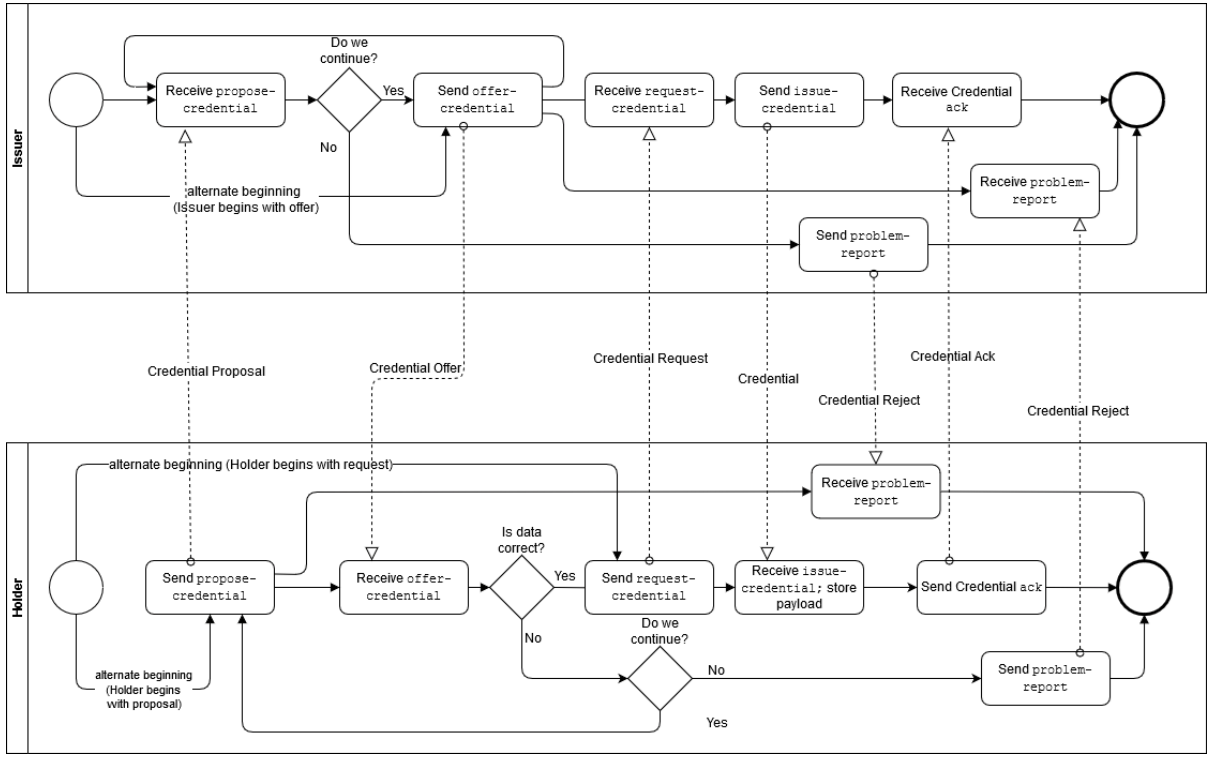


Candidates

- DIDComm
- OpenID for Verifiable Credential Issuance
- ISO 23220-3
- VC API

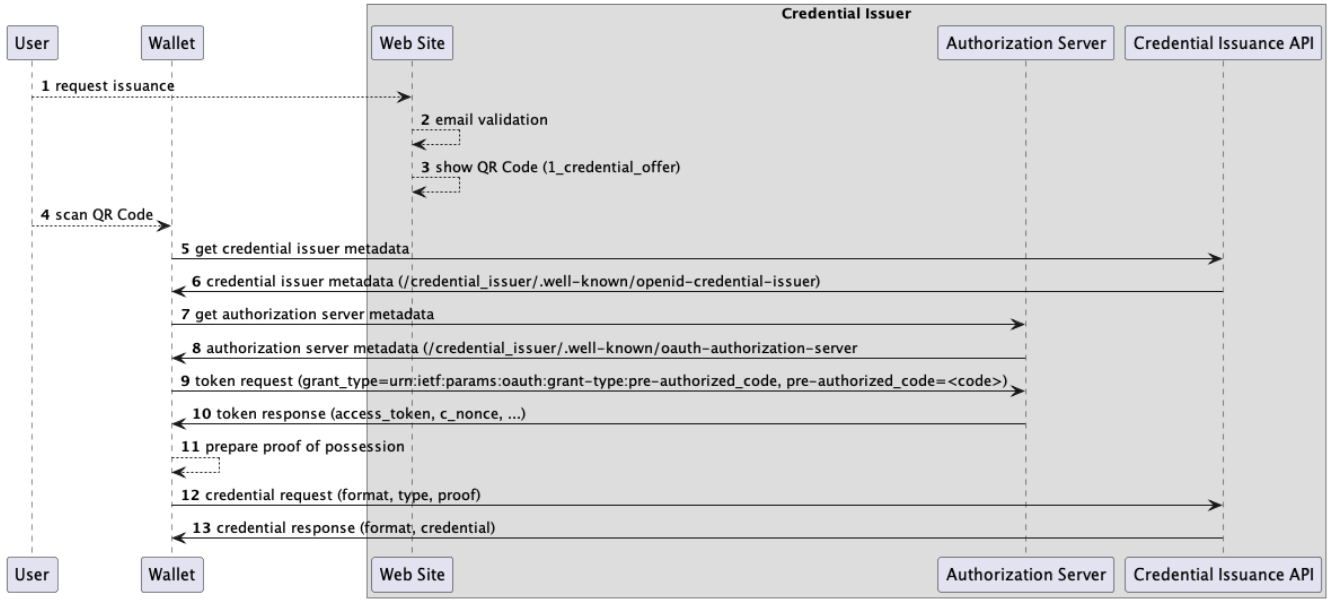
DIDComm Issue Credential Protocol 3.0

- Credential Issuance built on top of DIDComm
  - DIDComm is a generic, message-based, end-2-end secured communication protocol based on DIDs
- Credential format agnostic
- Batch issuance for credentials in different format but same claims
- Issuer communicates to user through Wallet
- Specification: Decentralized Identity Foundation



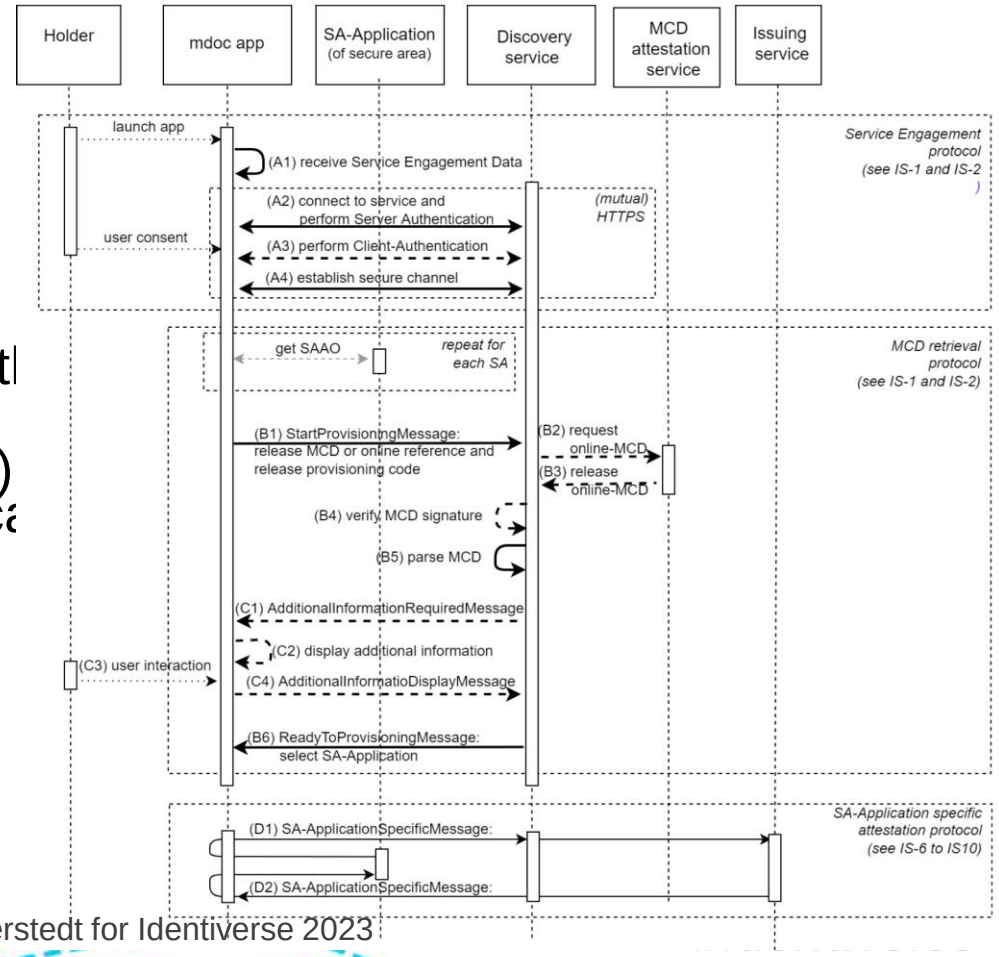
OpenID for Verifiable Credential Issuance (OID4VCI)

- OAuth protected API
  - leverages existing grant types and advanced OAuth security mechanisms (e.g. FAPI)
  - can be built on top of existing OpenID Connect implementations
  - issuer has ability to control UX to authenticate and identify end-user
- Credential format agnostic
- Supports different security levels
- Modular, supports different flows and trust mechanisms
- Batch issuance, deferred issuance
- Specification: OpenID Foundation
- Adopted by eIDAS v2 ARF



ISO 23220-3

- Message based protocol between mdoc app and mdoc issuer
- mdoc format specific
- Designed for high assurance credentials & issuer controlled process
- Generic base protocol + sub protocols for actual issuance:
  - BasicSA: mdoc App to Issuer communication wit attestation
  - HPKE-SA: Issuer to Secure Area (on the device) communication through mdoc App, connection c re-establish
    - Alternatively also supports OID4VCI
- Specification: ISO
- 23220 family cited in eIDAS v2 ARF



VC API

- RESTful API for Verifiable Credential Lifecycle Management
- Includes issuance support
- JSON LD specific
- Abstraction within a party, e.g. an issuer
- Interface to Wallet including user authentication and consent is implemented using other mechanisms, e.g OID4VCI (https://github.com/w3c-ccg/vc-api/issues/48)
- Specification: W3C CCG

Credential Exchange Protocols Comparison Matrix

https://docs.google.com/spreadsheets/d/1_KKQZmmNRnEME96fZCPbMW-TC9j0tQ-dVuk5zzKa8U8/edit#gid=1209461468

	Criteria	Issue Credential v2	OpenID4VCI	ISO 23220-3	VC API
ABOUT	Specification link and versioning	Version 2: https://github.com/hyperledger/aries-rfcs/blob/main/features/0453-issue-credential-v2/README.md	Latest Draft: https://openid.bitbucket.io/connect/openid-4-verifiable-credential-issuance-1_0.html		
	Specification Status	**Status of Issue Credential v2** - Aries Issue Credential v2 is a stable specification with ongoing development and improvement. - It is in an ACCEPTED status in the Aries project: https://github.com/hyperledger/aries-rfcs/blob/main/features/0453-issue-credential-v2/README.md **Status of DIDComm v2** - TBA	- OpenID4VCI is currently in draft status, and changes to the specification may be expected. - The OpenID Foundation (OIDF) is responsible for developing and maintaining the specification. - The OIDF has a well-established process for reviewing and updating the specification, which involves input from the community and security experts.		
	Specification Body	- Built on top of the DIDComm (DIF) and Hyperledger frameworks, which provide standardized messaging and decentralized identity management capabilities. - Decentralized Identity Foundation (DIF) is a young organisation and not yet widely known - DIDComm v3 might be intended for IETF	- OpenID Foundation (OIDF) - The OpenID Foundation (OIDF) is responsible for developing and maintaining the OpenID4VCI specification. - The OIDF has a well-established process for reviewing and updating the specification, which involves input from the community and security experts.	- ISO 18013-5 is an international standard backed by the International Organization for Standardization (ISO). It has a dedicated community of experts and stakeholders who work together to develop and maintain the standard. - The community may not be as accessible or open to developers as open-source communities.	- VC API is an open-source protocol. - The community provides resources, t developers integrate and use the protc
	Profile Objective(s)	- Issue Credential v2 protocol is a standard protocol that enables asynchronous secure exchanges of verifiable credentials between an Issuer and a Holder. - Designed to provide interoperability between the two parties, to protect the privacy of credential holders, and to enable the Holder to become a Prover in the sister RFC, 0454: Present Proof Protocol 2.0.	- Narrow focus on the lightweight issuance of personal identity credentials - Based on OAuth 2.0 protocol - Supports a range of credential formats, including verifiable credentials - Provides a standard approach to presenting and verifying credentials in different contexts, including online and in-person transactions	- Specifically designed for creating, issuing, and verifying mobile driver's licenses (mDL). - Provides a secure and standardized framework for governments and transportation authorities to issue digital driver's licenses to citizens, allowing them to store and present their licenses on their smartphones.	- VC API is an interoperable protocol fo - It is designed to work with different d networks and supports different crede verifiable credentials.
	OSS/IPR	- Open-source and provides protection through the DIF and Hyperledger foundations. - The Aries Issue Credential (RFC 0453), the DIF Credential Manifest and DIF Presentation Exchange specifications are all open source software. - The Aries Issuance flow (Aries RFC 0453) is released under the Apache License 2.0, which allows users to freely use, modify, and share the software. The DIF Credential Manifest and DIF Presentation Exchange specifications are released under the Creative Commons Attribution 4.0 International License, which allows users to freely use, modify, and share the software.	- OpenID4VCI is maintained by the OpenID Foundation (OIDF) as an open standard.	- ISO 18013-5 itself is a copyrighted document by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and it is not open source. - While the standard itself is not open source, it is possible that open-source projects or libraries may be developed to help implement the guidelines and requirements specified in ISO 18013-5. These open-source projects would have their own licenses and terms of use, separate from the ISO 18013-5 standard.	
USE CASES	Use Case Flexibility	- Highly flexible and can be used for various use cases across different domains. - It supports customizable verifiable credential formats and offers privacy-preserving mechanisms such as zero-knowledge proofs.	- It provides a standard approach to presenting and verifying credentials in different contexts, including online and in-person transactions. - OpenID4VCI supports a range of credential formats, including verifiable credentials, enabling interoperability between different systems and use cases.	- Focused on mobile driver's licenses and government-issued identification cards. - It has limited use case flexibility outside of the intended domain.	- VC API is highly flexible and can be u across different domains. - It supports customizable verifiable cr privacy-preserving mechanisms such a
	Additional Features	- Designed to be easily extensible and flexible, with a client that can be customized to support different use cases and workflows.	- Native to decentralized identity and verifiable credentials - Provides a mechanism for issuers to provide verifiable claims to holders that are compatible with OpenID Connect, simplifying integration with existing identity solutions. - Offers standard protocols and APIs for different use cases, including credential issuance and presentation, which are designed to work together in a flexible, interoperable manner.		
	Support for Additional Trust Tasks	Post issuance comm from issuer (from DIDComm perspective vs 1-time event)			
	Offline/Online Support				
	Designed for Mobile Device Use				
		- Aries Issue Credential v2 is a mature protocol with a wide deployment base	- Recently introduced protocol with a limited deployment base	- ISO 18013-5 is a mature standard with widespread adoption, particularly for mobile driver's licenses and electronic ID documents\	- VC API is a relatively new protocol, bu adoption in the decentralized identity

Part 4: “Holder Binding”

Andrew Hughes
Director of Identity Standards, Ping Identity

Who is the Holder and what are they Bound to?

- If I present a digital credential or document to Torsten, how does he know that the credential is about me? Or that I'm authorized to present it?
- And, how could I present somebody else's credential? ☺

What is “holder binding”?

Loosely translated:

“Is the credential presenter authorized to present the credential?”

“Is the entity that was originally issued the credential the subject of the credential?”

“Is the current holder of the credential the subject of the credential?”

“Does the subject of the credential control the keys/proofs for the credential?”

What are some definitions?

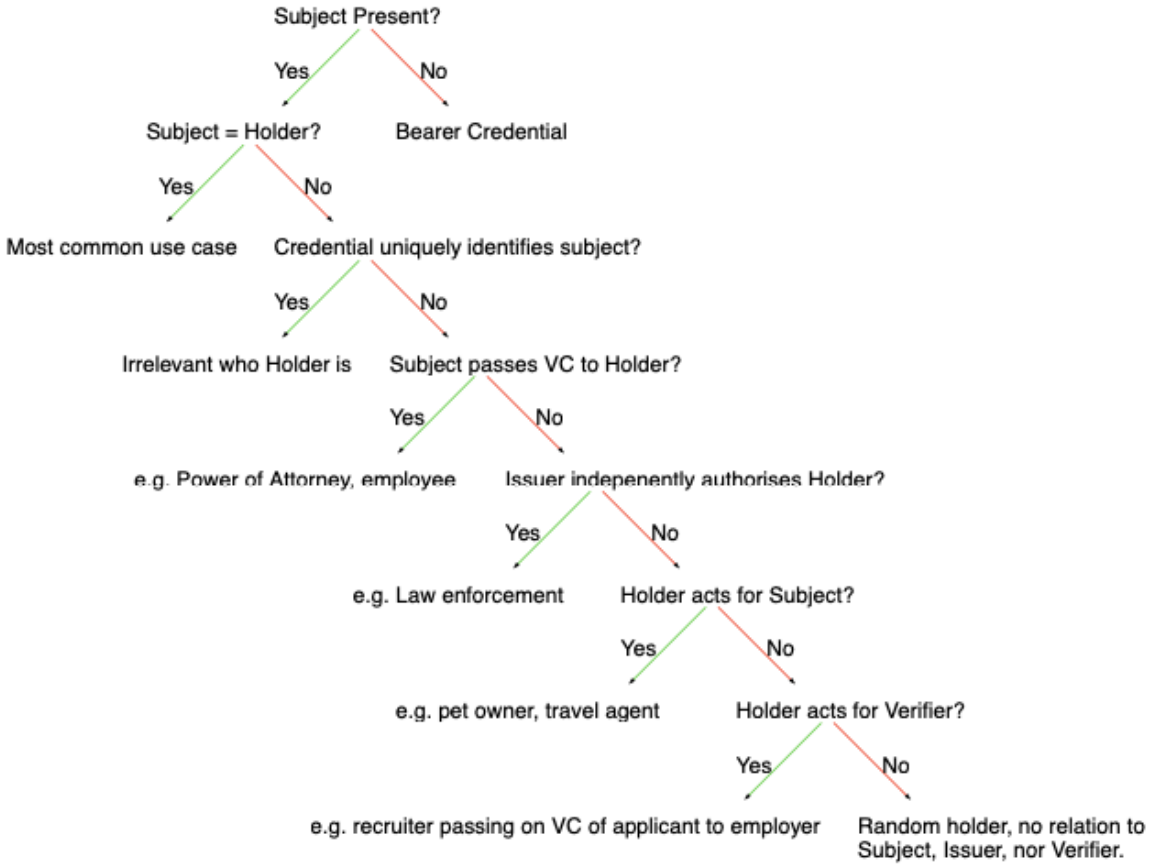


Figure 13 Subject-Holder Relationships in Verifiable Credentials.

A simple “solution”

- Simply have the user log in, and use the roles database to inform the credential verifier how to understand this
- Oh… wait…

The nature of the problem

- The semantics of the relationship between the credential, the contained claims and the original recipient, the entity associated with the claims, the subject of the credential, the holder of the credential, the presenter…
- Is defined by the issuer of the credential
- And because the verifier is not supposed to have a pre-established relationship with issuers, the verifier cannot ask the issuer about those relationships

What to do?

- Create a heavy, rich credential relationship policy management framework?
- Declare a single way to handle holder and subject relationship?
- Require tight integration between issuer and verifier?
- Declare how the relationship shall be interpreted within a family of credential standards & ensure protocols can convey this information.

Some mechanisms

- Proof of possession of a private key
- Assumption that the wallet/device has a user lock enabled
- Co-presentation of corroborating identification credential
- Biometric matching by the verifier (oversharing! yikes!)

OpenID for Verifiable Credential Issuance

- Describes three kinds of holder binding
  - Cryptographic, claim-based, biometrics-based
- Optional
- Two cryptographic binding options
  - Key material plus proof of control (proof includes sub_jwk or did)
  - Proof of control only (proof does not include sub_jwk or did)
- Support indicated in issuer's metadata parameters

ISO 23220 and ISO 18013 family

- ISO 18013-5 for mobile driving license states that credential Holder is defined as the credential Subject
- “Credential Holder Verification” – Verifier can signal to the mdoc app to execute a verification means that was authorized by the issuer, and to include the result as a data attribute in the response payload
- ISO 23220-3 (Issuance) will include the mechanism for authorization of verification means

Further reading

- Bastian, P., Joosten, R., Rivai, Z., Terbu, O., Edwin, S. Antonino, A., Fotiou, N., Curran, S., and Azeem, A. (2023). **Identifier Binding: defining the Core of Holder Binding**. Rebooting the Web of Trust XI. Retrieved from https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/final-documents/identifier-binding.pdf
- Terbu, O (2023). **Confirmation Method**. Presentation to W3C CCG. Retrieved from https://docs.google.com/presentation/d/1-uPVyl3S-vPvy4HqL6BcjN0xTu9AvqxFfwowqwzcXpo/edit
- **Credential Profile Comparison Matrix** https://docs.google.com/spreadsheets/d/1X93ptJcmfX1NZEo5E7ElnqJ-knDS4Dj6JOYSJ_2PsUw
- **OpenID for Verifiable Credentials Issuance** https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- **OpenID for Verifiable Presentations** https://openid.net/specs/openid-4-verifiable-presentations-1_0-ID2.html


THANK YOU!