OASIS LVCSP TC Response to the Private Identity and CVS Comments on LVCS CSD01

April 25, 2025

Reference:

Private Identity LLC and CVS Health Comments on OASIS Lightweight Verifiable Credential (LWVC) Schema Version 1.0
Committee Specification Draft 01 • 10 February 2025

Comment	Disposition of Comment	Action
Overall Assessment and Recommendations The Lightweight Verifiable Credential (LWVC) Specification provides a robust technical framework for creating and managing lightweight verifiable credentials. We commend the committee's attention to privacy-enhancing features such as selective disclosure and its progress toward aligning with globally recognized data protection principles. In order to further strengthen the specification, we recommend several enhancements that address data minimization, purpose limitation, explicit user consent, and alignment with international privacy and data protection frameworks such as GDPR, CCPA, HIPAA, and BIPA. The specific recommendations below are intended to reinforce the specification's technical rigor while ensuring that implementers can maintain compliance with diverse regulatory requirements and industry best practices. By integrating these modifications, the LWVC can become a model specification that strikes an optimal balance between innovation, interoperability, and individual privacy protections.	The LVCS document is intended to provide "templates" for schemas containing claims that are potentially widely useful. It is not intended to specify a VC ecosystem or framework for creating, operating or managing VCs. A generalized distributed identity framework was described in order to place the schemas into a context. Some of the proposed material is out of scope for Version 1 of the LVCS standard. Some additional material along the lines suggested could be added to a future Version 2.	Acknowledged No change

1. Data Minimization & Purpose Limitation **Recommendation:** Enforce strict data minimization by clearly identifying the minimal set of data required for each use case. Templates—especially those with broad coverage, such as the Expanded Personal Identity Schema (Template 5)—should be refined to ensure that only the essential data are collected and disclosed, and that the collection of any additional data is contingent upon explicit user consent. **Implementation Guidance:** 1. **Explicit Guidelines on Data Minimization**: Publish supplementary materials that instruct implementers on configuring identity credential templates so as to capture only essential data points. This ensures that any additional or optional fields are deliberately included and consented to. 2. **Principle of Least Privilege**: Encourage developers of wallet applications and credential-verification platforms to adopt an authorization model that requires minimal privileges for data access. 3. **Granular, Informed Consent**: Provide user interfaces and backend mechanisms for securing user consent at the level of specific data attributes, rather than requiring a blanket consent for large sets of personal data.	The templated schemas in this document are not intended to map directly to a specific use case or industry vertical. The proposed schemas provide different flavors of "KYC" – ranging from basic age verification to significant sets of identification claims. The goal is to have a minimum set of data (claims) for each template. It is expected that some use cases will require a combination of different VCs. For example, a university may request a basic identity matching VC prior to supplying its own VC for graduation status or a transcript. Combinations of VCs could be used to meet another service provider's VP requirements. Further guidance for schema implementors and users could be considered for Version 2.	No change
2. Enhanced Handling and Protection of Sensitive Data **Recommendation:** Strengthen the specification's guidelines around the storage and transfer of sensitive data, such as biometric information or health-related data (e.g., COVID-19 test results, vaccination records), to ensure robust encryption, access control, audit capabilities, and privacy-preserving cryptographic techniques.	Treatment of sensitive data in claims is for future study. Storage of claim data is not viewed as a schema-related consideration but could be reviewed for Version 2. Schema support for the encryption of claims is for future consideration.	Out of scope for Version 1. No change.

Implementation Guidance: 1. **Robust Encryption Protocols**: Incorporate modern encryption standards (e.g., AES-256 or other quantum-resistant algorithms when available) for data both in transit and at rest, ensuring that sensitive data remain confidential throughout their lifecycle. 2. **Secure Key Management and Audit Logging**: Require secure key management practices, with periodic rotation of encryption keys to mitigate breach risks. Implement thorough logging of all credential issuance, storage, and disclosure events. 3. **Privacy-Enhancing Technologies**: Encourage using zero-knowledge proofs, homomorphic tokenization, or advanced cryptographic techniques to verify sensitive attributes without exposing underlying raw data. 4. **Local, On-Device Processing**: Where feasible, biometric matching and other sensitive data processing should occur on the user's device, reducing the risk of centralized data breaches.	Zero-knowledge proofs derived from the templated schemas should be possible with the proposed templates.	
3. Explicit User Consent, Control, and Transparency **Recommendation:** Mandate explicit requirements for obtaining informed and granular user consent. Provide clear guidance on data retention, deletion, and correction to ensure that end users understand how their information is stored, used, and can be managed. **Implementation Guidance:** 1. **User Control Mechanisms**: Wallet applications should provide intuitive, user-friendly interfaces that enable individuals to manage their credentials, select which attributes to disclose, and revoke previously granted permissions.	This topic would be a policy, governance and systems design consideration. User consent could be considered at two points in the VC lifecycle: • A KYC Credential Issuer must interact with the Subject/User to identify the claims the User would allow to be included in a VC and what validation evidence would be provided. The Issuer cannot create a VC if the User does not consent to its creation.	Out of scope for a VC schema. No change

2. **Transparent Data Use**: Provide details regarding data retention periods and how data can be corrected or deleted in accordance with privacy laws such as GDPR or CCPA. 3. **Consent Framework References**: Include explicit references to applicable national and international privacy regulations to help implementers ensure compliance and build user trust.	• A Holder must consent to provide the Service Provider with specific VCs or Claims as part of a VP. Granularity of consent for presentations would not be specified in a schema. Data management specifications such as retention periods, wallet security, etc. would be external to the schema and most likely would be covered by governance policies.	
4. Mitigation of Data Linkage and Correlation Risks **Recommendation:** Address the risk that widely adopted, interoperable credential schemas could inadvertently enable cross-service correlation of personal data, increasing the potential for profiling or universal tracking. **Implementation Guidance:** 1. **Pseudonymous or Anonymous Identifiers**: Encourage or require the use of pseudonymous or anonymous identifiers, scoping these identifiers to specific contexts or relying parties to limit the accumulation of a universal tracking profile. 2. **Rotating GUIDs and DIDs**: Where feasible, rotate globally unique identifiers (GUIDs) or decentralized identifiers (DIDs) on a per-transaction basis to reduce the likelihood of cross-service correlation. 3. **Scoped Credentials**: Offer guidance on using different credential schemas or sub-credentials for discrete contexts (e.g., healthcare vs. financial services) to further protect user privacy.	Mechanisms and capabilities for reducing cross-service correlation and profiling via widely used schemas is for further study. This standard does not provide guidance for implementations within a given scope. This standard relates to basic KYC for an individual. It does not present a general model for VCs and does not cover special contexts such as medical records.	No change
5. Addressing Privacy Risks in the Event of Data Breaches	A VC schema does not address beaches of an implementation, other than perhaps with	Out of scope No change

Recommendation: Augment the security considerations section to more directly address the privacy implications of data breaches, particularly for high-risk categories of personal data such as medical records or biometrics. **Implementation Guidance:** 1. **Breach Notification Protocols**: Advise implementers to follow relevant legal frameworks (GDPR, CCPA, or regional equivalents) to ensure prompt and transparent breach notifications. 2. **Encryption and Tokenization**: Emphasize robust encryption, homomorphic tokenization, and secure storage solutions as foundational elements that reduce the impact of a breach by rendering exfiltrated data unusable. 3. **Incident Response**: Recommend that implementers adopt or reference standardized incident response protocols (e.g., ISO/IEC 27035).	respect to the choice of claims to include in the VC.	
6. Explicit Alignment with Global Privacy Regulations **Recommendation:** Insert additional language within the LWVC Specification highlighting that implementations must adhere to relevant global privacy statutes and regulations, such as GDPR, CCPA, HIPAA, or BIPA. **Implementation Guidance:** 1. **Regulatory Alignment**: Ensure that references to purpose limitation, data minimization, and individuals' rights to erasure and correction (where legally mandated) are embedded in the specification. 2. **Coordinated Compliance**: Provide mapping or cross-reference documentation that shows how LWVC aligns with established data protection standards and frameworks.	It might be possible to add statements in the standard to indicate that legal requirements and regulations take precedence over the selection of the templates to use. It is probably more important that such guidance be included in governance documents and policy samples than in a schema definition. Definitions for privacy terminology do not need to be included in this standard.	For future study No change

3. **Harmonized Terminology**: Clarify the definitions and usage of terms such as “data subject,” “personal data,” “processor,” and “controller,” consistent with key global regulatory instruments.		
7. Recommend Adding an Addendum for Healthcare-Specific Extensions and Use-Case **Recommendation:** Develop specialized healthcare extensions or templates (e.g., for patient registration, prescription fulfillment, telehealth authentication) that align with healthcare data models (e.g., HL7 FHIR) and address healthcare-specific privacy and interoperability requirements. **Implementation Guidance:** 1. **HL7 FHIR Integration**: Extend credential schemas to map to existing FHIR-based systems and EHR (electronic health record) workflows. 2. **Use-Case Examples**: Provide detailed examples illustrating how verifiable credentials can be used in healthcare scenarios, from booking appointments to filling prescriptions. 3. **Regulatory Consistency**: Ensure alignment with HIPAA, BIPA, and state-specific regulations for handling medical data, focusing on patient consent and purpose limitation.	The current standard is intended for use by Verifiers who wish to check the correctness of VCs and Claims – it does not cover data elements that relate to specific functions in specific industries such as healthcare. The application of VCs to specific use-case applications is out of scope. Note: Mapping to HL7 FHIR VC transfer requirements is complex and goes beyond what would be called “lightweight” and is subject to national variations. In the USA HL7 aims to follow NIST SP800-63.	Out of scope for Version 1 but possibly for future study.
8. Integration of Industry-Specific Guidelines for eKYC **Recommendation:** Update Section 4.3 to explicitly include references to industry-specific frameworks and guidelines, spanning healthcare, finance, and relevant European regulations. **Implementation Guidance:**	Explicit reference to industry-specific “frameworks” or practices is not needed for the purposes of this standard which aims to be widely useful across verticals. This standard is not intended to produce templates specific to each industry. There may, however, be value in developing	For future study Added references to Section 4.3

1. **Healthcare**: Incorporate HL7 FHIR US.IDENTITY-MATCHING guidance. 2. **Financial Services**: Add references to FFIEC guidance, FIDO Alliance initiatives, and Financial Services Identity standards. 3. **European Regulatory Environment**: Incorporate the EU PSC2 regulatory framework, ensuring alignment with European financial regulations and data protection mandates. 4. **Holistic Approach**: Tie these frameworks to existing technical standards such as ISO/IEC 18013-5, SD-JWT, and W3C Verifiable Credentials Data Model (VC DM) to cultivate a cohesive, multi-industry approach to identity verification.	supplemental material that maps the proposed templates to cover each of the frameworks for KYC (i.e. customer matching).	
Section-Specific Assessments and Recommendations Below are our detailed observations and proposed updates for specific sections of the LWVC Specification.	Noted.	
Section 1.2.2 Acronyms and Abbreviations **Recommendation:** Add the following term and definition: ● **Credential Service Provider (CSP):** A broader term than Credential Issuer (CI) that typically refers to the platform or service supporting the entire lifecycle of digital credentials—including issuing, storing, managing, and verifying credentials—according to NIST 800-63. **Rationale:** This expanded term aligns with widely recognized digital identity standards and clarifies how credential issuance services may also handle data storage, key management, user authentication, and credential verification.	Note that the terms and descriptions are informative and do not impact the actual schema templates that are specified. As a general comment, this standard did not aim to be fully consistent with the NIST SP800-63 terminology. This standard selected the term “service provider” to represent the party that receives identity claims and decides whether to provide specific services to the “buyer.” The term Credential Service Provider was not used in order to avoid confusion. And a definition for the VC platform is also not included.	For further study for Version 2. The definitions for Identity Provider and Credential Issuer have been updated. The Biometrics Credential Issuer definition has been added.

	A Credential Issuer is considered to be a “party” that can play one or more “roles” in the VC lifecycle, including validation of evidence, supply of biometrics data, etc. Future study can include identifying which widely recognized standards are being referred to by the comment.	
Section 2.3.3.1 Identity Credential Issuer **Recommendation:** Revise definitions to better reflect the language of NIST 800-63 regarding identity assurance. Specifically: ● **Credential Service Provider (CSP):** An entity that manages the complete lifecycle of digital credentials, including issuing, storing, updating, revoking, and facilitating the secure presentation of credentials. The CSP ensures that these credentials are created and maintained in a secure, standardized, and interoperable manner, consistent with industry best practices and applicable regulatory requirements. ● **Identity Provider (IdP):** An entity that authenticates users and asserts their identity. It verifies user credentials—often employing multi-factor authentication or other proofing methods—and issues identity assertions or tokens that relying parties use to grant access to digital services or resources. Though an IdP may overlap functionally with a CSP in some implementations, NIST 800-63 focuses on identity proofing, authentication, and issuance of identity assertions, not on the IdP label specifically.	See previous comments on Section 1.2.2. The definition for CSP is not the same as the previous one. Further study is needed to determine if the CSP does perform all of these functions (at least in our current model). Further rationalization of the CSP, IdP, BP (biometrics provider) and CI terms can be considered for Version 2 of the standard.	For further study for Version 2 of this standard. The definitions for Identity Provider and Credential Issuer have been modified. The Biometrics Credential Issuer definition has been added. See also the previous item.

Note: A service provider may combine IdP and CSP functions into a single system, but the terminology and approach may differ among different identity frameworks.		
Section 2.3.3.2 Biometric Credential Issuer **Recommendation:** Expand the description as follows: **Biometric Credential Issuer:** A specialized Credential Issuer that generates biometric information, creates biometric templates, and issues biometric claims or credentials. Government agencies issuing biometric passports, private companies offering facial recognition-based services, and other similar entities can act as Biometric Credential Issuers. This function can be part of a broader CSP role or a standalone service. **Additional Biometric Recommendations:** 1. **Data Minimization, Consent, & Purpose Limitation**: Clearly articulate the need for explicit user consent and specify that biometric data should only be collected for legitimate, narrowly defined purposes. 2. **Advanced Cryptographic Techniques**: Encourage the use of homomorphic tokenization, zero-knowledge proofs, or related technologies to enable verification without revealing raw biometric data. 3. **Local, On-Device Processing**: Favor decentralized, on-device processing of biometric data whenever possible to minimize large-scale data breach risks.	A definition for the role of “biometrics provider” should be added to clause 1. Clause 2.3.3.2 could be expanded to reference government agencies.	Accepted in part. A definition for a Biometrics Credential Issuer has been added to Clause 1.
Section 2.3.5.1 Platform-based Wallet **Recommendation:** Expand the definition to emphasize security measures. For example:	Current text in 2.3.5.1 can be expanded to provide more emphasis on security measures.	Accepted. Content of 2.3.5.1 has been updated

“A Platform Provider can optionally offer wallet-like functions as an alternative to, or in cooperation with, the Holder’s device. Platform-based wallets may facilitate the acquisition, storage, and management of verifiable credentials (VCs) and play a critical role in securing these credentials. These wallets should incorporate robust authentication mechanisms, such as password/PIN and biometric unlock, to ensure that verifiable presentations are generated only by the rightful owner. Secure wallet implementations are foundational to building trust in digital identity ecosystems.”		
Section 2.4.1 Biometric Verifiable Credentials **Recommendation:** Acknowledge and incorporate the multi-part binary structure of CBEFF (Common Biometric Exchange Formats Framework) when describing how biometric credentials fit into the LWVC context. Below is an example JSON-LD mapping to illustrate how CBEFF fields can be represented as claims in verifiable credentials: "@context": ["https://www.w3.org/2018/credentials/v1", { "cbeff": "https://example.org/cbeff#", "biometricIdentifier": "cbeff:biometricIdentifier", "biometricFeature": "cbeff:biometricFeature", "validityPeriod": "cbeff:validityPeriod", "creator": "cbeff:creator",	It is for further study how to incorporate the CBEFF multi-part structure into the LVCS context. V1 of the LVCS standard has intentionally excluded JSON-LD as an option. The additional guidance is for further study.	An appendix has been added to the standard to introduce CBEFF.

<pre>"index": "cbeff:index",
"challengeResponse":
"cbeff:challengeResponse",
"payload": "cbeff:payload"
}
]</pre>
Further Guidance:
● **Encoding**: Binary data such as raw biometric payloads should be base64-encoded for JSON compatibility.
● **Security**: Digital signatures, proof blocks, and additional cryptographic assurances should be included to ensure the authenticity and integrity of biometric data.
● **Modality-specific Extensions**: Allow additional specialized fields for different biometric modalities (iris, voice, gait, etc.) without modifying the core structure.		

Section 2.6 VC Assurance Levels **Recommendation:** Remove the current definitions of “Issuer Assurance Level,” “User Assurance Level,” and “Credential Assurance Level,” and adopt the NIST SP 800-63 terminology of **Identity** Assurance Level (IAL). This realignment will ensure consistency with recognized digital identity frameworks and reduce confusion around the meaning of assurance levels. **Rationale:** ● **Consistency with NIST 800-63**: Many U.S. federal and state regulations (21 CFR Part 1311, 49 CFR § 580.3, OMB M-04-04) align with NIST SP 800-63 for identity proofing and authentication guidelines.	Revisions to Clause 2.6 are needed to provide greater alignment with NIST SP 800. This document does not aim to provide a full explanation of assurance management. The goal is to identify the required claims or metadata that need to be included in the templates. Accommodation of assurance levels might be beyond the level of a “lightweight” VC.	Accepted. Section 2.6 has been updated.

• **Healthcare**: HL7 FHIR US.IDENTITY-MATCHING guidance also aligns with NIST 800-63 definitions of assurance. • **Global Compatibility**: Reduces friction for implementers who must meet multiple regulatory requirements.		
Section 4.3 Standards for eKYC VCs **Recommendation:** Enhance the discussion around industry-specific standards for electronic Know Your Customer (eKYC) processes, making explicit references to: • **Healthcare**: HL7 FHIR US.IDENTITY-MATCHING guidance. • **Financial Services**: FFIEC guidance, FIDO Alliance frameworks, and Financial Services Identity initiatives. • **European Regulatory Environment**: Incorporate guidance on EU PSC2 for payment services. Additionally, emphasize the inclusion of explicit user consent, control, and transparency in eKYC processes.	Additional references from the selected verticals could be added but close alignment of the templates to specific industry standards is not the goal of this standard.	References to industry standards have been added.
Section 5 Templates for eKYC Schemas **Recommendation:** Promote data minimization and selective disclosure across all schema templates. In particular, the Extended Personal Identity Schema (Template 5) should be refined to reduce the risk of over-collecting personal data. **Alignment:** • **HL7 FHIR US.IDENTITY-MATCHING** • **FFIEC** • **FIDO Alliance and Financial Services Identity**	LVCS supports data minimization by endorsing several templates that use only a small selection of the IANA-registered claims. Implementation of the schemas using SD is allowed. An SP/Verifier that has specified it needs one template will need to determine if a user-selected subset of claims is acceptable. Further discussion of Template 5 may be useful. There may not be any eKYC use-	No change

• **EU PSC2** This ensures minimal data collection with explicit user consent, following best practices in privacy and security.	cases that require all of Template 5 claims. However, if the Holder wishes to have a "comprehensive" set of claims to select from, they might choose to work with a CI to create a T5 VC.	
Recommended LWVC Schema Templates Below, we propose specific modifications to the existing LWVC templates to consolidate overlapping schemas, simplify implementation, and embed privacy-first design principles.	Noted	
Recommend Combining Template 1, 3, 4, and 5 – Personal Identity Schema This comprehensive schema captures core personal identity information while preserving the principle of data minimization through optional fields. By combining Templates 1, 3, 4, and 5, implementers have a single, flexible schema that can scale from basic identity use cases to more complex applications (healthcare, finance, etc.) without encouraging the over-collection of data. **Key Benefits:** • **Simplification**: A single reference schema reduces development overhead and streamlines interoperability. • **Privacy by Design**: Optional fields allow implementers to include only the minimal necessary data for a specific use case, consistent with best practices and global privacy regulations. • **Interoperability**: Shared mandatory fields ensure consistency, while optional fields cater to specialized industry needs. **Additional Biometric Extension:** For legacy or high-assurance scenarios involving biometric	For further study and possible refinement in Version 2, based on implementor feedback. One goal of LVCS was to NOT have optional fields. T1, T3 and T4 are subsets of T5 and could easily be folded into a full template but this would necessitate allowing optional fields. Is the reduction in the number of distinct templates a useful goal? The comment references "shared mandatory fields" for the purpose of interoperability. Would the choice of mandatory fields not be basically the same as creating specialized templates? Note that the concept of templates is not intended to be mapped to specific verticals.	Not accepted. No change.

data, include an optional `biometric_templates` array aligned with CBEFF structures, ensuring robust handling and privacy controls.		

Below is the proposed combined schema with explanatory comments.
 	
{
"$schema": "http://json-schema.org/draft-07/schema#",
"title": "Personal Identity Schema Template",
"description": "This schema defines the Personal Identity Schema Template for Lightweight Verifiable Credential Schema Version 1.0, Committee Specification Draft 02.",
"type": "object",
"properties": {
"sub": {
"type": "string",
"description": "A unique identifier for the End-User. Contains a GUID (anonymized) from the CSP and includes no PII."
},
"given_name": {
"type": "array",
"description": "One or more first names matching official identity evidence.",
"items": { "type": "string" }
},
"family_name": {
	This is based on an older json-schema version.
	Some elements of this could be used.
	This is basically a combination template except for T2.
	It does not restrict itself to IANA registered claims and does not seem to be “lightweight”.
	Do we want names, emails, etc. to be arrays?
		For future consideration as noted above.

"type": "array",
"description": "One or more last names matching official identity evidence.",
"items": { "type": "string" }
},
"phone_number": {
"type": "array",
"description": "One or more phone numbers. If no mobile number is available, an alternative may be provided.",
"items": { "type": "string" }
},
"email": {
"type": "array",
"description": "One or more email addresses. Verification status may be stored separately or as additional metadata.",
"items": { "type": "string", "format": "email" }
},
"birthdate": {
"type": "string",
"description": "The End-User's date of birth.",
"format": "date"
},
"address": {
"type": "array",
"description": "An array of preferred postal addresses.",
"items": {
"type": "object",		

"properties": {
"formatted": { "type": "string" },
"street_address": { "type": "string" },
"locality": { "type": "string" },
"region": { "type": "string" },
"postal_code": { "type": "string" },
"country": { "type": "string" }
},
"required": ["formatted", "country"]
}
},
"assurance_level": {
"type": "string",
"description": "A URL or reference to the verification level (e.g., IAL 1, IAL 2). Aligns with NIST SP 800-63A."
},
"updated_at": {
"type": "string",
"description": "Timestamp of the last credential update.",
"format": "date-time"
},
"previousCredential": {
"anyOf": [
{ "type": "string" },
{ "type": "null" }
],
"description": "Reference to an earlier credential (if any) to maintain continuity."		

```
    },

    /* Optional Fields */
    "issuer": {
      "type": "string",
      "description": "Credential Service
Provider (CSP) issuing this credential."
    },
    "assurance_type": {
      "type": "string",
      "description": "The standard used for
assurance (e.g., NIST SP 800-63.4)."
    },
    "assurance_evidence": {
      "type": "string",
      "description": "Link to evidence
supporting the stated assurance level."
    },
    "birth_place": {
      "type": "object",
      "description": "City, state/province,
and country of birth.",
      "properties": {
        "city": { "type": "string" },
        "state": { "type": "string" },
        "country": { "type": "string" }
      },
      "required": ["city", "country"]
    },
    "admin_gender": {
      "type": "string",
```

```
      "description": "Gender as recorded on
official documents.",
      "enum": ["Male", "Female", "X",
"Other", "Not Specified"]
    },
    "citizenship": {
      "type": "string",
      "description": "The End-User's country
of citizenship."
    },
    "country_of_residence": {
      "type": "string",
      "description": "The country or state
where the End-User lives."
    },
    "face_portrait": {
      "type": "string",
      "description": "URL to the user's
facial image, conforming to ISO 19794-5
standards.",
      "format": "uri"
    },
    "biometric_token": {
      "type": "string",
      "description": "A homomorphic token
derived from the user's biometric data."
    },
    "overthreshold_13": { "type": "boolean"
},
    "overthreshold_18": { "type": "boolean"
},
```

```
    "overthreshold_21": { "type": "boolean"
},
    "overthreshold_25": { "type": "boolean"
},
    "overthreshold_65": { "type": "boolean"
},
    "legal_name": {
      "type": "string",
      "description": "The official, full
legal name of the End-User."
    },
    "middle_name": {
      "type": "array",
      "items": { "type": "string" }
    },
    "nickname": { "type": "string" },
    "preferred_username": { "type": "string"
},
    "profile": {
      "type": "string",
      "format": "uri"
    },
    "website": {
      "type": "string",
      "format": "uri"
    },
    "zoneinfo": { "type": "string" },
    "locale": { "type": "string" },
    "phone_number_verified": {
      "type": "boolean",
      "description": "Indicates if the phone
number was verified."
```

```
    },
    "service_provider_identifier": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "identifier_type": { "type":
"string" },
          "identifier_value": { "type":
"string" }
        },
        "required": ["identifier_type",
"identifier_value"]
      }
    },
    "credential_card": {
      "type": "array",
      "description": "Array representing
various credential cards (e.g., driver's
licenses).",
      "items": {
        "type": "object",
        "properties": {
          "card_type": { "type": "string" },
          "holder_name": { "type": "string"
},
          "date_of_birth": { "type":
"string", "format": "date" },
          "unique_identifier": { "type":
"string" },
          "issuing_authority": { "type":
"string" },
```

<pre>"issue_date": { "type": "string", "format": "date" },
"expiration_date": { "type": "string", "format": "date" },
"photo_url": { "type": "string", "format": "uri" },
"additional_info": {
"type": "array",
"items": {
"type": "object",
"additionalProperties": true
}
}
},
"required": [
"card_type",
"holder_name",
"unique_identifier",
"issuing_authority",
"issue_date"
]
}
},
"biometric_templates": {
"type": "array",
"description": "Optional array of biometric templates reflecting CBEFF structures.",
"items": {
"type": "object",
"properties": {</pre>		

"biometricIdentifier": { "type": "string" },
"biometricFeature": { "type": "string" },
"validityPeriod": {
"type": "object",
"properties": {
"start": { "type": "string", "format": "date-time" },
"end": { "type": "string", "format": "date-time" }
},
"required": ["start", "end"]
},
"creator": { "type": "string" },
"index": { "type": "string" },
"challengeResponse": { "type": "string" },
"payload": { "type": "string" }
}
}
}
},
"required": [
"sub",
"given_name",
"family_name",
"phone_number",
"email",
"birthdate",
"address",
"assurance_level",		

<pre>"updated_at",
"previousCredential"
]
}</pre>		

Template 2 – Basic Age Disclosure Schema
Discussion:
This simplified schema attests to certain age thresholds (e.g., over 13, 18, 21, 25, 65) without disclosing additional PII such as full name, address, or birthdate. It provides privacy-preserving proof of age for scenarios like purchasing age-restricted products or verifying parental consent, relying on digital signatures and secure wallet frameworks for verification.
Mandatory Fields:
● **sub (or "subject")**: A GUID or unique identifier.
● **overthreshold_X** booleans (13, 18, 21, 25, 65) to indicate the subject's eligibility without revealing exact age.
● **updated_at** for version control.
● **previousCredential** for audit trail.
Optional Fields (e.g., **issuer**, **assurance_type**, **face_portrait**, **birthdate**) support more complex scenarios but remain non-essential for basic age verification.
 	
<pre>{
"$schema": "http://json-schema.org/draft-07/schema#",
"title": "Basic Age Disclosure Schema",
"description": "A schema to prove age without revealing additional PII. The credential attests to the subject's age using</pre>
	Contains optional and null claims. If optional claims are included, then SD would be needed to ensure only consented elements go to the SD.
	Consideration should be given to a very basic VC that the Holder can simply consent to delivering to the SP with little or no need for processing within the wallet.
		For discussion and acceptance.

boolean indicators for specific age thresholds. The verifiable presentation must be cryptographically sound and originate from the rightful holder via digital signatures.",
"type": "object",
"properties": {
"sub": {
"type": "string",
"description": "A unique identifier for the End-User. Contains a GUID provided by the Credential Service Provider (CSP) and includes no PII."
},
"overthreshold_13": {
"type": "boolean",
"description": "True if the End-User is over 13."
},
"overthreshold_18": {
"type": "boolean",
"description": "True if the End-User is over 18."
},
"overthreshold_21": {
"type": "boolean",
"description": "True if the End-User is over 21."
},
"overthreshold_25": {
"type": "boolean",
"description": "True if the End-User is over 25."		

```
    },
    "overthreshold_65": {
      "type": "boolean",
      "description": "True if the End-User is
over 65."
    },
    "updated_at": {
      "type": "string",
      "format": "date-time",
      "description": "A timestamp
representing the last update to the
credential."
    },
    "previousCredential": {
      "anyOf": [
        { "type": "string" },
        { "type": "null" }
      ],
      "description": "Either null or a
reference to the unique identifier (sub) of a
prior credential. This creates an audit trail
to show that the new credential is a revised
version of an earlier one."
    },

    /* Optional Fields */
    "issuer": {
      "type": "string",
      "description": "The Credential Service
Provider (CSP) that issued the credential."
    },
    "assurance_type": {
```

"type": "string",
"description": "The standard used for assurance (e.g., NIST SP 800-63.4)."
},
"assurance_evidence": {
"type": "string",
"description": "A URL or reference to additional evidence supporting the stated assurance level."
},
"face_portrait": {
"type": "string",
"format": "uri",
"description": "A URL linking to a picture of the End-User's face. Should conform to ISO 19794-5/INCITS 385-2004 (S2019) standards. Contains PII."
},
"biometric_identity_token": {
"type": "string",
"description": "The End-User's homomorphic token derived from biometric data, used to enhance identity verification without exposing raw biometric data."
},
"birthdate": {
"type": "string",
"format": "date",
"description": "The End-User's date of birth. This field is optional to protect PII."
}		

<pre> },
  "required": [
    "sub",
    "overthreshold_13",
    "overthreshold_18",
    "overthreshold_21",
    "overthreshold_25",
    "overthreshold_65",
    "updated_at",
    "previousCredential"
  ]
}</pre>		

Concluding Remarks We respectfully request that OASIS review these comments and consider integrating the recommended modifications into the *Lightweight Verifiable Credential Schema Version 1.0, Committee Specification Draft 01*. Incorporating the proposed refinements will bolster the specification's privacy posture, align it more closely with recognized global standards (NIST 800-63, GDPR, CCPA, HIPAA, BIPA, etc.), and ensure that LWVC becomes a future-proof, interoperable standard in the evolving digital identity landscape. **Key Takeaways** 1. **Data Minimization**: Embed strong guidance on the principle of least privilege and user consent. 2. **Privacy-by-Design**: Encourage advanced cryptographic approaches (e.g., zero-knowledge proofs, homomorphic encryption) to protect raw data. 3. **Explicit Assurance Levels**: Harmonize assurance definitions with NIST SP 800-63 to reduce confusion and improve alignment with regulatory frameworks.	Noted. Items here have been addressed in the detailed comments. <u>Notes</u> 1. Accepted 2. Relationship between the schema and data encryption is to be elaborated. 3. Accepted. How assurance levels are propagated needs to be made clearer as well. 4. Rejected. The goal was not to create use-case specific templates. 5. Rejected. How this should be reflected in VC schemas needs to be elaborated.	No changes proposed for this comment.

4. **Industry-Specific Extensions**: Provide targeted templates and references (HL7 FHIR, FFIEC, FIDO, PSC2) for healthcare, finance, and other regulated sectors. 5. **Biometric Safeguards**: Strengthen requirements around biometric data handling, ensuring local processing, user consent, and minimal data exposure. We understand that our suggestions may require additional effort to integrate. We look forward to volunteering to support the Committee, and welcome opportunities to collaborate further in refining these proposals. Thank you for your time and consideration.		