|  |  |
| --- | --- |
|  | T. Lodderstedt |
|  | D. Fett |
|  | yes.com |
|  | July 16, 2019 |

**OpenID Connect for Identity Assurance 1.0  
openid-connect-4-identity-assurance-1\_0-06**

# [Abstract](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.abstract)

This specification defines an extension of OpenID Connect for providing Relying Parties with verified Claims about End-Users. This extension is intended to be used to verify the identity of a natural person in compliance with a certain law.

# [Table of Contents](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.toc)

* **1.** [**Introduction**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.1)
  + **1.1.** [**Terminology**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.1.1)
* **2.** [**Scope and Requirements**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.2)
* **3.** [**Claims**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.3)
  + **3.1.** [**Additional Claims about End-Users**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.3.1)
  + **3.2.** [**txn Claim**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.3.2)
* **4.** [**Verified Data Representation**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4)
  + **4.1.** [**verification Element**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1)
    - **4.1.1.** [**Evidence**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1.1)
  + **4.2.** [**claims Element**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.2)
* **5.** [**Requesting Verified Claims**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5)
  + **5.1.** [**Requesting End-User Claims**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5.1)
  + **5.2.** [**Requesting Verification Data**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5.2)
  + **5.3.** [**Defining constraints on Verification Data**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5.3)
* **6.** [**Examples**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6)
  + **6.1.** [**id\_document**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.1)
  + **6.2.** [**id\_document + utility bill**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.2)
  + **6.3.** [**Notified eID system (eIDAS)**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.3)
  + **6.4.** [**Verified Claims in UserInfo Response**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.4)
    - **6.4.1.** [**Request**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.4.1)
    - **6.4.2.** [**UserInfo Response**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.4.2)
  + **6.5.** [**Verified Claims in ID Tokens**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.5)
    - **6.5.1.** [**Request**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.5.1)
    - **6.5.2.** [**ID Token**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.5.2)
  + **6.6.** [**Aggregated Claims**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.6)
  + **6.7.** [**Distributed Claims**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.7)
* **7.** [**OP Metadata**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.7)
* **8.** [**Transaction-specific Purpose**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.8)
* **9.** [**Privacy Consideration**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.9)
* **10.** [**Security Considerations**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.10)
* **11.** [**Predefined Values**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11)
  + **11.1.** [**Trust Frameworks**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11.1)
  + **11.2.** [**Identity Documents**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11.2)
  + **11.3.** [**Verification Methods**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11.3)
* **12.** [**JSON Schema**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.12)
* **13.** [**References**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.references)
  + **13.1.** [**Normative References**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.references.1)
  + **13.2.** [**Informative References**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.references.2)
* **Appendix A.** [**Acknowledgements**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.appendix.A)
* **Appendix B.** [**Notices**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.appendix.B)
* **Appendix C.** [**Document History**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.appendix.C)
* [**Authors' Addresses**](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.authors)

# [1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.1) [Introduction](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#Introduction)

This specification defines an extension to OpenID Connect [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID) to address the use case of strong identity verification of a natural person in accordance with certain laws. Examples include Anti Money Laundering Laws, Telecommunication Acts, Anti Terror Laws, and regulations on trust services, such as eIDAS [[eIDAS]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#eIDAS).

In such use cases, the Relying Parties (RPs) need to know the assurance level of the Claims about the End-User attested by the OpenID Connect Providers (OPs) or any other trusted source along with evidence related to the identity verification process.

The acr Claim, as defined in Section 2 of the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID), is suited to attest information about the authentication performed in a OpenID Connect transaction. But identity assurance requires a different representation for the following reason: authentication is an aspect of an OpenID Connect transaction while identity assurance is a property of a certain Claim or a group of Claims and several of them will typically be conveyed to the RP as the result of an OpenID Connect transaction.

For example, the assurance an OP typically will be able to attest for an e-mail address will be “self-asserted” or “verified by opt-in or similar mechanism”. The family name of a user, in contrast, might have been verified in accordance with the respective Anti Money Laundering Law by showing an ID Card to a trained employee of the OP operator.

Identity assurance therefore requires a way to convey assurance data along with and coupled to the respective Claims about the End-User. This specification proposes a suitable representation and mechanisms the RP will utilize to request verified claims about an End-User along with identity assurance data and for the OP to represent these verified Claims and accompanying identity assurance data.

# [1.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.1.1) [Terminology](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#terminology)

This section defines some terms relevant to the topic covered in this documents, heavily inspired by NIST SP 800-63A [[NIST-SP-800-63a]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#NIST-SP-800-63a).

* Identity Proofing - process in which a user provides evidence to an OP or claim provider reliably identifying themselves, thereby allowing the OP to assert that identification at a useful identity assurance level.
* Identify Verification - process conducted by the OP or a claim provider to verify the user's identity.
* Identity Assurance - process in which the OP or a claim provider attests identity data of a certain user with a certain assurance towards a RP, typically expressed by way of an assurance level. Depending on legal requirements, the OP may also be required to provide evidence of the identity verification process to the RP.
* Verified Claims - Claims about an End-User, typically a natural person, whose binding to a particular user account were verified in the course of an identity verification process.

# [2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.2) [Scope and Requirements](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#scope-and-requirements)

The scope of the extension is to define a mechanism to assert verified Claims, in general, and to introduce new Claims about the End-User required in the identity assurance space; one example would be the place of birth.

The RP will be able to request the minimal data set it needs (data minimization) and to express requirements regarding this data and the evidence and the identity verification processes employed by the OP.

This extension will be usable by OPs operating under a certain regulation related to identity assurance, such as eIDAS notified eID systems, as well as other OPs. Strictly regulated OPs can attest identity data without the need to provide further evidence since they are approved to operate according to well-defined rules with clearly defined liability.

For example in the case of eIDAS, the peer review ensures eIDAS compliance and the respective member state takes the liability for the identities asserted by its notified eID systems. Every other OP not operating under such well-defined conditions is typically required to provide the RP data about the identity verification process along with identity evidence to allow the RP to conduct their own risk assessment and to map the data obtained from the OP to other laws. For example, it shall be possible to use identity data maintained in accordance with the Anti Money Laundering Law to fulfill requirements defined by eIDAS.

From a technical perspective, this means this specification allows the OP to attest verified Claims along with information about the respective trust framework (and assurance level) but also supports the externalization of information about the identity verification process.

The representation defined in this specification can be used to provide RPs with verified Claims about the End-User via any appropriate channel. In the context of OpenID Connnect, verified Claims can be attested in ID Tokens or as part of the UserInfo response. It is also possible to utilize the format described here in OAuth Token Introspection responses (see [[RFC7662]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#RFC7662) and [[I-D.ietf-oauth-jwt-introspection-response]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#I-D.ietf-oauth-jwt-introspection-response)) to provide resource servers with verified Claims.

This extension is intended to be truly international and support identity assurance for different and across jurisdictions. The extension is therefore extensible to support additional trust frameworks, verification methods, and identity evidence.

In order to give implementors as much flexibility as possible, this extension can be used in conjunction with existing OpenID Connect Claims and other extensions within the same OpenID Connect assertion (e.g., ID Token or UserInfo response) utilized to convey Claims about End-Users.

For example, OpenID Connect [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID) defines Claims for representing family name and given name of a user without a verification status. Those Claims can be used in the same OpenID Connect assertion beside verified Claims represented according to this extension.

In the same way, existing Claims to inform the RP of the verification status of the phone\_number and email Claims can be used together with this extension.

Even for asserting verified Claims, this extension utilizes existing OpenID Connect Claims if possible and reasonable. The extension will, however, ensure RPs cannot (accidentally) interpret unverified Claims as verified Claims.

# [3.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.3) [Claims](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#claims)

# [3.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.3.1) [Additional Claims about End-Users](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#userclaims)

In order to fulfill the requirements of some jurisdictions on identity assurance, this specification defines the following Claims for conveying user data in addition to the Claims defined in the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID):

* place\_of\_birth: a structured Claim representing the End-User’s place of birth. It consists of the following fields:
  + country: [[ISO3166-1]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#ISO3166-1) Alpha-2 (e.g., DE) or [[ISO3166-3]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#ISO3166-3)
  + region: State, province, prefecture, or region component
  + locality: city or other locality
* nationality: represents the user’s nationality in format [[ISO3166-1]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#ISO3166-1) Alpha-2, e.g., DE
* birth\_family\_name: family name someone has when he or she is born, or at least from the time he or she is a child. This term can be used by a person who changes the family name later in life for any reason.
* birth\_given\_name: given name someone has when he or she is born, or at least from the time he or she is a child. This term can be used by a person who changes the given name later in life for any reason.
* birth\_middle\_name: middle name someone has when he or she is born, or at least from the time he or she is a child. This term can be used by a person who changes the middle name later in life for any reason.
* salutation: End-User’s salutation, e.g. “Mr.”
* title: End-User’s title, e.g. “Dr.”

# [3.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.3.2) [txn Claim](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#txn-claim)

Strong identity verification typically requires the participants to keep an audit trail of the whole process.

The txn Claim as defined in [[RFC8417]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#RFC8417) is used in the context of this extension to build audit trails across the parties involved in an OpenID Connect transaction.

If the OP issues a txn, it MUST maintain a corresponding audit trail, which at least consists of the following details:

* the transaction id,
* the authentication methods employed, and
* the transaction type (e.g. scope values).

This transaction data MUST be stored as long as it is required to store transaction data for auditing purposes by the respective regulation.

The RP requests this Claim like any other Claim via the claims parameter or as part of a default Claim set identified by a scope value.

The txn value MUST allow an RP to obtain these transaction details if needed.

Note: the mechanism to obtain the transaction details from the OP and their format is out of scope of this specification.

# [4.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4) [Verified Data Representation](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#verified-data-representation)

This extension to OpenID Connect wants to ensure that RPs cannot mix up verified and unverified Claims and incidentally process unverified Claims as verified Claims.

The representation proposed therefore provides the RP with the verified Claims within a container element verified\_claims. This container is composed of the verification evidence related to a certain verification process and the corresponding Claims about the End-User which were verified in this process.

This section explains the structure and meaning of verified\_claims in detail. A machine-readable syntax definition is given as JSON schema in [Section 12](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#json_schema). It can be used to automatically validate JSON documents containing a verified\_claims element.

verified\_claims consists of the following sub-elements:

* verification: REQUIRED. Object that contains all data about the verification process.
* claims: REQUIRED. Object that is the container for the verified Claims about the End-User.

Note: implementations MUST ignore any sub-element not defined in this specification or extensions of this specification.

# [4.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1) [verification Element](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#verification)

This element contains the information about the process conducted to verify a person's identity and bind the respective person data to a user account.

The verification element consists of the following elements:

trust\_framework: REQUIRED. String determing the trust framework governing the identity verification process and the identity assurance level of the OP.

An example value is eidas\_ial\_high, which denotes a notified eID system under eIDAS [[eIDAS]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#eIDAS) providing identity assurance at level of assurance "High".

An initial list of standardized values is defined in [Trust Frameworks](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values_tf). Additional trust framework identifiers can be introduced [how?]. RPs SHOULD ignore verified\_claims claims containing a trust framework id they don't understand.

The trust\_framework value determines what further data is provided to the RP in the verification element. A notified eID system under eIDAS, for example, would not need to provide any further data whereas an OP not governed by eIDAS would need to provide verification evidence in order to allow the RP to fulfill its legal obligations. An example of the latter is an OP acting under the German Anti-Money laundering law (de\_aml).

date: Time stamp in ISO 8601:2004 [[ISO8601-2004]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#ISO8601-2004) YYYY-MM-DD format representing the date when identity verification took place. Presence of this element might be required for certain trust frameworks.

verification\_process: Unique reference to the identity verification process as performed by the OP. Used for backtracing in case of disputes or audits. Presence of this element might be required for certain trust frameworks.

Note: While id refers to the identity verification process at the OP, the txn claim refers to a particular OpenID Connect transaction in which the OP attested the user's verified identity data towards a RP.

evidence is a JSON array containing information about the evidence the OP used to verify the user's identity as separate JSON objects. Every object contains the property type which determines the type of the evidence. The RP uses this information to process the evidence property appropriately.

Important: implementations MUST ignore any sub-element not defined in this specification or extensions of this specification.

# [4.1.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1.1) [Evidence](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#evidence)

The following types of evidence are defined:

* id\_document: verification based on any kind of government issued identity document
* utility\_bill: verification based on a utility bill
* qes: verification based on a eIDAS Qualified Electronic Signature

# [4.1.1.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1.1.1) [id\_document](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#id-document)

The following elements are contained in an id\_document evidence sub-element.

method: REQUIRED. The method used to verify the id document. Predefined values are given in [Verification Methods](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values_vm)

verifier: OPTIONAL. A JSON object denoting the legal entity that performed the identity verification on behalf of the OP. This object SHOULD only be included if the OP did not perform the identity verification itself. This object consists of the following properties:

* organization: String denoting the organization which performed the verification on behalf of the OP.
* agent: Agent (person) who conducted the verification. The agent may be identified by Name or an identifier which can be resolved into the agent’s name during an audit.

document: A JSON object representing the id document used to perform the id verification. It consists of the following properties:

* type: REQUIRED. String denoting the type of the id document. Standardized values are defined in [Identity Documents](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values_idd). The OP MAY use other than the predefined values in which case the RPs will either be unable to process the assertion, just store this value for audit purposes, or apply bespoken business logic to it.
* number: String representing the number of the identity document.
* issuer: A JSON object containg information about the government agency that issued this identity document. This object consists of the following properties:
  + name: REQUIRED. Designation of the issuer of the identity document
  + country: String denoting the country where the document was issued, format: ISO 3166-1 Alpha-2, e.g. "DE".
* date\_of\_issuance: REQUIRED if this attribute exists for the particular type of document. The date the document was issued as ISO 8601:2004 YYYY-MM-DD format.
* date\_of\_expiry: REQUIRED if this attribute exists for the particular type of document. The date the document will expire as ISO 8601:2004 YYYY-MM-DD format.

# [4.1.1.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1.1.2) [utility\_bill](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#utility-bill)

The following elements are contained in a utility\_bill evidence sub-element.

provider: REQUIRED. A JSON object identifying the respective provider that issued the bill. The object consists of the following properties:

* name: A String designating the provider.
* All elements of the OpenID Connect address Claim ([[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID))

date: A ISO 8601:2004 YYYY-MM-DD formatted string containing the date when this bill was issued.

# [4.1.1.3.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1.1.3) [qes](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#qes)

The following elements are contained in a qes evidence sub-element.

issuer: REQUIRED. A String denoting the trust service provider that created the eletronic signatue.

issued\_at: REQUIRED. The date the signature was created as ISO 8601:2004 YYYY-MM-DD format

serial\_number: REQUIRED. String containing the serial number of the certificate used to sign.

# [4.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.2) [claims Element](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#claimselement)

The claims element contains the claims about the End-User which were verified by the process and according to the policies determined by the corresponding verification element.

The claims element MAY contain one or more of the following Claims as defined in Section 5.1 of the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID)

* name
* given\_name
* middle\_name
* family\_name
* birthdate
* address

or the claims defined in [Section 3.1](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#userclaims).

The claims element MAY also contain other claims given the value of the respective claim was verified in the verification process represented by the sibling verification element.

# [5.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5) [Requesting Verified Claims](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#requesting-verified-claims)

# [5.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5.1) [Requesting End-User Claims](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#req_claims)

Verified Claims can be requested on the level of individual Claims about the End-User by utilizing the claims parameter as defined in Section 5.5. of the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID).

verified\_claims is added to the userinfo or id\_token element of the claims parameter.

Since verified\_claims contains the effective Claims about the End-User in a nested claims element, the syntax is extended to include expressions on nested elements as follows. The verified\_person\_data element includes a claims element, which in turn includes the desired Claims as keys with a null value. An example is shown in the following:

{

"userinfo":{

"verified\_claims":{

"claims":{

"given\_name":null,

"family\_name":null,

"birthdate":null

}

}

}

}

Use of the claims parameter allows the RP to exactly select the Claims about the End-User needed for its use case. This extension therefore allows RPs to fulfill the requirement for data minimization.

RPs MAY indicate that a certain Claim is essential to the successful completion of the user journey by utilizing the essential field as defined in Section 5.5.1. of the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID). The following example designates both given as well as family name as being essential.

{

"userinfo":{

"verified\_claims":{

"claims":{

"given\_name":{"essential": true},

"family\_name":{"essential": true},

"birthdate":null

}

}

}

}

This specification introduces the additional field purpose to allow a RP to state the purpose for the transfer of a certain End-User Claim it is asking for. The field purpose can be a member value of each individually requested Claim, but a Claim cannot have more than one associated purpose.

purpose OPTIONAL. String describing the purpose for obtaining a certain End-User Claim from the OP. The purpose MUST NOT be shorter than 3 characters or longer than 300 characters. If this rule is violated, the authentication request MUST fail and the OP returns an error invalid\_request to the RP. The OP MUST display this purpose in the respective user consent screen(s) in order to inform the user about the designated use of the data to be transferred or the authorization to be approved. If the parameter purpose is not present in the request, the OP MAY display a value that was pre-configured for the respective RP. For details on UI localization see [Section 8](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#purpose).

Example:

{

"userinfo":{

"verified\_claims":{

"claims":{

"given\_name":{

"essential":true,

"purpose":"To make communication look more personal"

},

"family\_name":{

"essential":true

},

"birthdate":{

"purpose":"To send you best wishes on your birthday"

}

}

}

}

}

Note: A claims sub-element with value null is interpreted as a request for all possible Claims. An example is shown in the following:

{

"userinfo":{

"verified\_claims":{

"claims":null

}

}

}

Note: The claims sub-element can be omitted, which is equivalent to a claims element whose value is null.

Note: If the claims sub-element is empty or contains a Claim not fulfilling the requirements defined in [Section 4.2](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#claimselement), the OP will abort the transaction with an invalid\_request error.

# [5.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5.2) [Requesting Verification Data](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#req_verification)

The content of the verification element is basically determined by the respective trust\_framework and the Claim source's policy.

This specification also defines a way for the RP to explicitly request certain data to be present in the verification element. The syntax is based on the rules given in [Section 5.1](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#req_claims) and extends them for navigation into the structure of the verification element.

Elements within verification can be requested in the same way as defined in [Section 5.1](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#req_claims) by adding the respective element as shown in the following example:

{

"verified\_claims":{

"verification":{

"date":null,

"evidence":null

},

"claims":null

}

}

It requests the date of the verification and the available evidence to be present in the issued assertion.

Note: the RP does not need to explicitly request the trust\_framework field as it is a mandatory element of the verified\_claims Claim.

The RP may also dig one step deeper into the structure and request certain data to be present within every evidence. A single entry is used as prototype for all entries in the result array:

{

"verified\_claims":{

"verification":{

"date":null,

"evidence":[

{

"method":null,

"document":null

}

]

},

"claims":null

}

}

This example requests the method element and the document element for every evidence available for a certain user account.

Note: the RP does not need to explicitly request the type field as it is a mandatory element of any evidence entry.

The RP may also request certain data within the document element to be present. This again follows the syntax rules used above.

{

"verified\_claims":{

"verification":{

"date":null,

"evidence":[

{

"method":null,

"document":{

"issuer":null,

"number":null,

"date\_of\_issuance":null

}

}

]

},

"claims":null

}

}

Note: the RP does not need to explicitly request the type field as it is a mandatory element of any document entry.

It is at the discretion of the Claim source to decide whether the requested verification data is provided to the RP.

# [5.3.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.5.3) [Defining constraints on Verification Data](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#constraintedclaims)

The RP MAY express requirements regarding the elements in the verification sub-element.

This, again, requires an extension to the syntax as defined in Section 5.5. of the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID) due to the nested nature of the verified\_claims claim.

Section 5.5.1 of the OpenID Connect specification [[OpenID]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID) defines a query syntax that allows for the member value of the Claim being requested to be a JSON object with additional information/constraints on the Claim. For doing so it defines three members (essential, value and values) with special query meanings and allows for other special members to be defined (while stating that any members that are not understood must be ignored).

This specification re-uses that mechanism and introduces a new such member max\_age (see below).

To start with, the RP MAY limit the possible values of the elements trust\_framework, evidence/type, evidence/method, and evidence/document/type by utilizing the value or values fields.

The following example shows that the RP wants to obtain an attestation based on AML and limited to users who were identified in a bank branch using government issued id documents.

{

"userinfo":{

"verified\_claims":{

"verification":{

"trust\_framework":{

"value":"de\_aml"

},

"evidence":[

{

"type":{

"value":"id\_document"

},

"method":{

"value":"pipp"

},

"document":{

"type":{

"values":[

"idcard",

"passport"

]

}

}

}

]

},

"claims":null

}

}

}

The RP MAY also express a requirement regarding the age of the verification data, i.e., the time elapsed since the verification process asserted in the verification element has taken place.

This specification therefore defines a new member max\_age.

max\_age: OPTIONAL. Is a JSON number value only applicable to Claims that contain dates or timestamps. It defines the maximum time (in seconds) to be allowed to elapse since the value of the date/timestamp up to the point in time of the request. The OP should make the calculation of elapsed time starting from the last valid second of the date value. The following is an example of a request for Claims where the verification process of the data is not allowed to be older than 63113852 seconds.

The following is an example:

{

"userinfo":{

"verified\_claims":{

"verification":{

"date":{

"max\_age":63113852

}

},

"claims":null

}

}

}

The OP SHOULD try to fulfill this requirement. If the verification data of the user is older than the requested max\_age, the OP MAY attempt to refresh the user’s verification by sending her through a online identity verification process, e.g. by utilizing an electronic ID card or a video identification approach.

If the OP is unable to fulfill the requirement (even in case it is marked as being essential), it will provide the RP with the data available and the RP may decide how to use the data. The OP MUST NOT return an error in case it cannot return all Claims requested as essential Claims.

# [6.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6) [Examples](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#examples)

The following sections show examples of verified\_claims.

The first and second section show JSON snippets of the general identity assurance case, where the RP is provided with verification evidence for different verification methods along with the actual Claims about the End-User.

The third section illustrates how the contents of this object could look like in case of a notified eID system under eIDAS, where the OP does not need to provide evidence of the identity verification process to the RP.

Subsequent sections contain examples for using the verified\_claims Claim on different channels and in combination with other (unverified) Claims.

# [6.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.1) [id\_document](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#id-document-1)

{

"verified\_claims":{

"verification":{

"trust\_framework":"de\_aml",

"date":"2013-02-21",

"verification\_process":"676q3636461467647q8498785747q487",

"evidence":[

{

"type":"id\_document",

"method":"pipp",

"document":{

"type":"idcard",

"issuer":{

"name":"Stadt Augsburg",

"country":"DE"

},

"number":"53554554",

"date\_of\_issuance":"2012-04-23",

"date\_of\_expiry":"2022-04-22"

}

}

]

},

"claims":{

"given\_name":"Max",

"family\_name":"Meier",

"birthdate":"1956-01-28",

"place\_of\_birth":{

"country":"DE",

"locality":"Musterstadt"

},

"nationality":"DE",

"address":{

"locality":"Maxstadt",

"postal\_code":"12344",

"country":"DE",

"street\_address":"An der Sanddüne 22"

}

}

}

}

# [6.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.2) [id\_document + utility bill](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#id-document-utility-bill)

{

"verified\_claims":{

"verification":{

"trust\_framework":"de\_aml",

"date":"2013-02-21",

"verification\_process":"676q3636461467647q8498785747q487",

"evidence":[

{

"type":"id\_document",

"method":"pipp",

"document":{

"document\_type":"de\_erp\_replacement\_idcard",

"issuer":{

"name":"Stadt Augsburg",

"country":"DE"

},

"number":"53554554",

"date\_of\_issuance":"2012-04-23",

"date\_of\_expiry":"2022-04-22"

}

},

{

"type":"utility\_bill",

"provider":{

"name":"Stadtwerke Musterstadt",

"country":"DE",

"region":"Thüringen",

"street\_address":"Energiestrasse 33"

},

"date":"2013-01-31"

}

]

},

"claims":{

"given\_name":"Max",

"family\_name":"Meier",

"birthdate":"1956-01-28",

"place\_of\_birth":{

"country":"DE",

"locality":"Musterstadt"

},

"nationality":"DE",

"address":{

"locality":"Maxstadt",

"postal\_code":"12344",

"country":"DE",

"street\_address":"An der Sanddüne 22"

}

}

}

}

# [6.3.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.3) [Notified eID system (eIDAS)](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#notified-eid-system-eidas)

{

"verified\_claims":{

"verification":{

"trust\_framework":"eidas\_ial\_substantial"

},

"claims":{

"given\_name":"Max",

"family\_name":"Meier",

"birthdate":"1956-01-28",

"place\_of\_birth":{

"country":"DE",

"locality":"Musterstadt"

},

"nationality":"DE",

"address":{

"locality":"Maxstadt",

"postal\_code":"12344",

"country":"DE",

"street\_address":"An der Sanddüne 22"

}

}

}

}

# [6.4.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.4) [Verified Claims in UserInfo Response](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#verified-claims-in-userinfo-response)

# [6.4.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.4.1) [Request](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#request)

In this example we assume the RP uses the scope parameter to request the email address and, additionally, the claims parameter, to request verified Claims.

The scope value is: scope=openid email

The value of the claims parameter is:

{

"userinfo":{

"verified\_claims":{

"claims":{

"given\_name":null,

"family\_name":null,

"birthdate":null

}

}

}

}

# [6.4.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.4.2) [UserInfo Response](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#userinfo-response)

The respective UserInfo response would be

HTTP/1.1 200 OK

Content-Type: application/json

{

"iss":"https://server.example.com",

"sub":"248289761001",

"email":"janedoe@example.com",

"email\_verified":true,

"verified\_claims":{

"verification":{

"trust\_framework":"de\_aml",

"date":"2013-02-21",

"verification\_process":"676q3636461467647q8498785747q487",

"evidence":[

{

"type":"id\_document",

"method":"pipp",

"document":{

"type":"idcard",

"issuer":{

"name":"Stadt Augsburg",

"country":"DE"

},

"number":"53554554",

"date\_of\_issuance":"2012-04-23",

"date\_of\_expiry":"2022-04-22"

}

}

]

},

"claims":{

"given\_name":"Max",

"family\_name":"Meier",

"birthdate":"1956-01-28"

}

}

}

# [6.5.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.5) [Verified Claims in ID Tokens](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#verified-claims-in-id-tokens)

# [6.5.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.5.1) [Request](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#request-1)

In this case, the RP requests verified Claims along with other Claims about the End-User in the claims parameter and allocates the response to the ID Token (delivered from the token endpoint in case of grant type code).

The claims parameter value is

{

"id\_token":{

"email":null,

"preferred\_username":null,

"picture":null,

"verified\_claims":{

"claims":{

"given\_name":null,

"family\_name":null,

"birthdate":null

}

}

}

}

# [6.5.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.5.2) [ID Token](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#id-token)

The respective ID Token could be

{

"iss":"https://server.example.com",

"sub":"24400320",

"aud":"s6BhdRkqt3",

"nonce":"n-0S6\_WzA2Mj",

"exp":1311281970,

"iat":1311280970,

"auth\_time":1311280969,

"acr":"urn:mace:incommon:iap:silver",

"email":"janedoe@example.com",

"preferred\_username":"j.doe",

"picture":"http://example.com/janedoe/me.jpg",

"verified\_claims":{

"verification":{

"trust\_framework":"de\_aml",

"date":"2013-02-21",

"verification\_process":"676q3636461467647q8498785747q487",

"evidence":[

{

"type":"id\_document",

"method":"pipp",

"document":{

"type":"idcard",

"issuer":{

"name":"Stadt Augsburg",

"country":"DE"

},

"number":"53554554",

"date\_of\_issuance":"2012-04-23",

"date\_of\_expiry":"2022-04-22"

}

}

]

},

"claims":{

"given\_name":"Max",

"family\_name":"Meier",

"birthdate":"1956-01-28"

}

}

}

# [6.6.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.6) [Aggregated Claims](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#aggregated-claims)

Note: line breaks for display purposes only

HTTP/1.1 200 OK

Content-Type: application/json

{

"iss":"https://server.example.com",

"sub":"248289761001",

"email":"janedoe@example.com",

"email\_verified":true,

"\_claim\_names":{

"verified\_claims":"src1"

},

"\_claim\_sources":{

"src1":{

"JWT":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJodHRwczovL3NlcnZlci5vdGh

lcm9wLmNvbSIsInZlcmlmaWVkX2NsYWltcyI6eyJ2ZXJpZmljYXRpb24iOnsidHJ1c3RfZnJhbWV3b3

JrIjoiZWlkYXNfaWFsX3N1YnN0YW50aWFsIn0sImNsYWltcyI6eyJnaXZlbl9uYW1lIjoiTWF4IiwiZ

mFtaWx5X25hbWUiOiJNZWllciIsImJpcnRoZGF0ZSI6IjE5NTYtMDEtMjgifX19.M8tTKxzj5LBgqGj

UAzFooEiCPJ4wcZVQDrnW5\_ooAG4"

}

}

}

# [6.7.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.6.7) [Distributed Claims](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#distributed-claims)

HTTP/1.1 200 OK

Content-Type: application/json

{

"iss":"https://server.example.com",

"sub":"248289761001",

"email":"janedoe@example.com",

"email\_verified":true,

"\_claim\_names":{

"verified\_claims":"src1"

},

"\_claim\_sources":{

"src1":{

"endpoint":"https://server.yetanotherop.com/claim\_source",

"access\_token":"ksj3n283dkeafb76cdef"

}

}

}

# [7.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.7) [OP Metadata](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#opmetadata)

The OP advertises its capabilities with respect to verified Claims in its openid-configuration (see [[OpenID-Discovery]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OpenID-Discovery)) using the following new elements:

verified\_claims\_supported: Boolean value indicating support for verified\_claims, i.e. the OpenID Connect for Identity Assurance extension.

trust\_frameworks\_supported This is a JSON array containing all supported trust frameworks.

evidence\_supported This JSON array contains all types of identity evidence the OP uses.

id\_documents\_supported This JSON array contains all identity documents utilized by the OP for identity verification.

id\_documents\_verification\_methods\_supported This element is a JSON array containing the id document verification methods a OP supports as defined in [Section 4.1](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#verification).

claims\_in\_verified\_claims\_supported This JSON array contains all claims supported within verified\_claims.

This is an example openid-configuration snippet:

{

...

"verified\_claims\_supported":true,

"trust\_frameworks\_supported":[

"nist\_800\_63A\_ial\_2",

"nist\_800\_63A\_ial\_3"

],

"evidence\_supported":[

"id\_document",

"utility\_bill",

"qes"

]

"id\_documents\_supported":[

"idcard",

"passport",

"driving\_permit"

]

"id\_documents\_verification\_methods\_supported":[

"pipp",

"sripp",

"eid"

]

"claims\_in\_verified\_claims\_supported":[

"given\_name",

"family\_name",

"birthdate",

"place\_of\_birth",

"nationality",

"address"

],

...

}

The OP MUST support the claims parameter and needs to publish this in its openid-configuration using the claims\_parameter\_supported element.

# [8.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.8) [Transaction-specific Purpose](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#purpose)

This specification introduces the request parameter purpose to allow a RP to state the purpose for the transfer of user data it is asking for.

purpose OPTIONAL. String describing the purpose for obtaining certain user data from the OP. The purpose MUST NOT be shorter than 3 characters and MUST NOT be longer than 300 characters. If these rules are violated, the authentication request MUST fail and the OP returns an error invalid\_request to the RP.

The OP MUST display this purpose in the respective user consent screen(s) in order to inform the user about the designated use of the data to be transferred or the authorization to be approved.

In order to ensure a consistent UX, the RP MAY send the purpose in a certain language and request the OP to use the same language using the ui\_locales parameter.

If the parameter purpose is not present in the request, the OP MAY utilize a description that was pre-configured for the respective RP.

Note: In order to prevent injection attacks, the OP MUST escape the text appropriately before it will be shown in a user interface. The OP MUST expect special characters in the URL decoded purpose text provided by the RP. The OP MUST ensure that any special characters in the purpose text cannot be used to inject code into the web interface of the OP (e.g., cross-site scripting, defacing). Proper escaping MUST be applied by the OP. The OP SHALL NOT remove characters from the purpose text to this end.

# [9.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.9) [Privacy Consideration](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#Privacy)

OP and RP MUST establish a legal basis before exchanging any personally identifiable information. It can be established upfront or in the course of the OpenID process.

# [10.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.10) [Security Considerations](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#Security)

The integrity and authenticity of the issued assertions MUST be ensured in order to prevent identity spoofing. The Claims source MUST therefore cryptographically sign all assertions.

The confidentiality of all user data exchanged between the protocol parties MUST be ensured using suitable methods at transport or application layer.

# [11.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11) [Predefined Values](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values)

# [11.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11.1) [Trust Frameworks](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values_tf)

This section defines trust framework identifiers for use with this specification.

|  |  |
| --- | --- |
| **Identifier** | **Definition** |
| de\_aml | The OP verifies and maintains user identities in conforms with the German Anti-Money Laundering Law. |
| eidas\_ial\_substantial | The OP is able to attest user identities in accordance with the EU regulation No 910/2014 (eIDAS) at the identitfication assurance level "Substantial". |
| eidas\_ial\_high | The OP is able to attest user identities in accordance with the EU regulation No 910/2014 (eIDAS) at the identitfication assurance level "High". |
| nist\_800\_63A\_ial\_2 | The OP is able to attest user identities in accordance with the NIST Special Publication 800-63A at the Identity Assurance Level 2. |
| nist\_800\_63A\_ial\_3 | The OP is able to attest user identities in accordance with the NIST Special Publication 800-63A at the Identity Assurance Level 3. |

# [11.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11.2) [Identity Documents](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values_idd)

This section defines identity document identifiers for use with this specification.

|  |  |
| --- | --- |
| **Identifier** | **Definition** |
| idcard | An identity document issued by a country's government for the purpose of identifying a citizen. |
| passport | A passport is a travel document, usually issued by a country's government, that certifies the identity and nationality of its holder primarily for the purpose of international travel.[[OxfordPassport]](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#OxfordPassport) |
| driving\_permit | Official document permitting an individual to operate motorized vehicles. In the absence of a formal identity document, a driver's license may be accepted in many countries for identity verification. |
| de\_idcard\_foreigners | ID Card issued by the German government to foreign nationals. |
| de\_emergency\_idcard | ID Card issued by the German government to foreign nationals as passports replacement |
| de\_erp | Electronic Resident Permit issued by the German government to foreign nationals |
| de\_erp\_replacement\_idcard | Electronic Resident Permit issued by the German government to foreign nationals as replacement for another identity document |
| de\_idcard\_refugees | ID Card issued by the German government to refugees as passports replacement |
| de\_idcard\_apatrids | ID Card issued by the German government to apatrids as passports replacement |
| de\_certificate\_of\_suspension\_of\_deportation | identity document issued to refugees in case of suspension of deportation that are marked as "id card replacement" |
| de\_permission\_to\_reside | permission to reside issued by the German governed to foreign nationals appliying for asylum |
| de\_replacement\_idcard | ID Card replacement document issued by the German government to foreign nationals (see Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory, Residence Act, Appendix D1 ID Card replacement according to § 48 Abs. 2 i.V.m. § 78a Abs. 4) |

# [11.3.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.11.3) [Verification Methods](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#predefined_values_vm)

This section defines verification method identifiers for use with this specification.

|  |  |
| --- | --- |
| **Identifier** | **Definition** |
| pipp | Physical In-Person Proofing |
| sripp | Supervised remote In-Person Proofing |
| eid | Online verification of an electronic ID card |

# [12.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.12) [JSON Schema](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#json_schema)

This section contains the JSON Schema of assertions containing the verified\_claims claim.

{

"$schema": "http://json-schema.org/draft-07/schema#",

"definitions":{

"qes":{

"type":"object",

"properties":{

"type":{

"type":"string",

"enum":[

"qes"

]

},

"issuer":{

"type":"string"

},

"issued\_at":{

"type":"string",

"format":"date"

},

"serial\_number":{

"type":"string"

}

},

"required": ["type","issuer","serial\_number","issued\_at"]

},

"utility\_bill":{

"type":"object",

"properties":{

"type":{

"type":"string",

"enum":[

"utility\_bill"

]

},

"provider":{

"type":"object",

"properties":{

"name":{

"type":"string"

},

"country":{

"type":"string"

},

"region":{

"type":"string"

},

"street\_address":{

"type":"string"

}

}

},

"date":{

"type":"string"

}

},

"required": ["type","provider","date"]

},

"id\_document":{

"type":"object",

"properties":{

"type":{

"type":"string",

"enum":[

"id\_document"

]

},

"method":{

"type":"string",

"enum":["pipp","sripp","eid"]

},

"verifier":{

"type":"object",

"properties":{

"organization":{

"type":"string"

},

"agent":{

"type":"string"

}

}

},

"document":{

"type":"object",

"properties":{

"type":{

"type":"string",

"enum":[

"idcard",

"passport",

"driving\_permit",

"de\_idcard\_foreigners",

"de\_emergency\_idcard",

"de\_erp",

"de\_erp\_replacement\_idcard",

"de\_idcard\_refugees",

"de\_idcard\_apatrids",

"de\_certificate\_of\_suspension\_of\_deportation",

"de\_permission\_to\_reside",

"de\_replacement\_idcard"

]

},

"number":{

"type":"string"

},

"issuer":{

"type":"object",

"properties":{

"name":{

"type":"string"

},

"country":{

"type":"string"

}

}

},

"date\_of\_issuance":{

"type":"string",

"format":"date"

},

"date\_of\_expiry":{

"type":"string",

"format":"date"

}

}

}

},

"required":[

"type",

"method",

"document"

]

}

},

"type":"object",

"properties":{

"verified\_claims":{

"type":"object",

"properties":{

"verification":{

"type":"object",

"properties":{

"trust\_framework":{

"type":"string",

"enum":[

"de\_aml",

"eidas\_ial\_substantial",

"eidas\_ial\_hig",

"nist\_800\_63A\_ial\_2",

"nist\_800\_63A\_ial\_3"

]

},

"date":{

"type":"string",

"format":"date"

},

"verification\_process":{

"type":"string"

},

"evidence":{

"type":"array",

"minItems": 1,

"items":{

"oneOf":[

{

"$ref":"#/definitions/id\_document"

},

{

"$ref":"#/definitions/utility\_bill"

},

{

"$ref":"#/definitions/qes"

}

]

}

}

},

"required":["trust\_framework"],

"additionalProperties": false

},

"claims":{

"type":"object",

"minProperties": 1

}

},

"required":["verification","claims"],

"additionalProperties": false

},

"txn": {"type": "string"}

},

"required":["verified\_claims"]

}

# [13.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.references) References

# [13.1.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.references.1) Normative References

|  |  |
| --- | --- |
| **[ISO3166-1]** | International Organization for Standardization, "[ISO 3166-1:1997. Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes](https://www.iso.org/standard/63545.html)", 2013. |
| **[ISO3166-3]** | International Organization for Standardization, "[ISO 3166-1:2013. Codes for the representation of names of countries and their subdivisions -- Part 3: Code for formerly used names of countries](https://www.iso.org/standard/63547.html)", 2013. |
| **[ISO8601-2004]** | International Organization for Standardization, "[ISO 8601:2004. Data elements and interchange formats - Information interchange - Representation of dates and times](http://www.iso.org/iso/catalogue_detail?csnumber=40874)", 2004. |
| **[OpenID]** | Sakimura, N., Bradley, J., Jones, M., de Medeiros, B. and C. Mortimore, "[OpenID Connect Core 1.0 incorporating errata set 1](http://openid.net/specs/openid-connect-core-1_0.html)", Nov 2014. |
| **[OpenID-Discovery]** | Sakimura, N., Bradley, J., de Medeiros, B. and E. Jay, "[OpenID Connect Discovery 1.0 incorporating errata set 1](https://openid.net/specs/openid-connect-discovery-1_0.html)", Nov 2014. |
| **[RFC8417]** | Hunt, P., Jones, M., Denniss, W. and M. Ansari, "[Security Event Token (SET)](https://tools.ietf.org/html/rfc8417)", RFC 8417, DOI 10.17487/RFC8417, July 2018. |

# [13.2.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.references.2) Informative References

|  |  |
| --- | --- |
| **[eIDAS]** | European Parliament, "[REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910)", July 2014. |
| **[I-D.ietf-oauth-jwt-introspection-response]** | Lodderstedt, T. and V. Dzhuvinov, "[JWT Response for OAuth Token Introspection](https://tools.ietf.org/html/draft-ietf-oauth-jwt-introspection-response-03)", Internet-Draft draft-ietf-oauth-jwt-introspection-response-03, May 2019. |
| **[NIST-SP-800-63a]** | NIST, Fentony, James., Lefkovitz, Naomi., Danker, Jamie., Choong, Yee-Yin., Greene, Kristen. and Mary. Theofanos, "[NIST Special Publication 800-63A, Digital Identity Guidelines, Enrollment and Identity Proofing Requirements](https://doi.org/10.6028/NIST.SP.800-63a)", June 2017. |
| **[OxfordPassport]** | Cane, P. and Mary. Conaghan, "[The New Oxford Companion to Law. ISBN 9780199290543.](http://www.oxfordreference.com/view/10.1093/acref/9780199290543.001.0001/acref-9780199290543-e-1616)", 2008. |
| **[RFC7662]** | Richer, J., "[OAuth 2.0 Token Introspection](https://tools.ietf.org/html/rfc7662)", RFC 7662, DOI 10.17487/RFC7662, October 2015. |

# [Appendix A.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.appendix.A) [Acknowledgements](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#Acknowledgements)

The following people at yes.com and partner companies contributed to the concept described in the initial contribution to this specification: Karsten Buch, Lukas Stiebig, Sven Manz, Waldemar Zimpfer, Willi Wiedergold, Fabian Hoffmann, Daniel Keijsers, Ralf Wagner, Sebastian Ebling, Peter Eisenhofer.

I would like to thank Sebastian Ebling, Marcos Sanz, Tom Jones, Mike Pegman, Michael B. Jones, and Jeff Lombardo for their valuable feedback that helped to evolve this specification.

# [Appendix B.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.appendix.B) [Notices](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#notices)

Copyright (c) 2019 The OpenID Foundation.

The OpenID Foundation (OIDF) grants to any Contributor, developer, implementer, or other interested party a non-exclusive, royalty free, worldwide copyright license to reproduce, prepare derivative works from, distribute, perform and display, this Implementers Draft or Final Specification solely for the purposes of (i) developing specifications, and (ii) implementing Implementers Drafts and Final Specifications based on such documents, provided that attribution be made to the OIDF as the source of the material, but that such attribution does not indicate an endorsement by the OIDF.

The technology described in this specification was made available from contributions from various sources, including members of the OpenID Foundation and others. Although the OpenID Foundation has taken steps to help ensure that the technology is available for distribution, it takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this specification or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any independent effort to identify any such rights. The OpenID Foundation and the contributors to this specification make no (and hereby expressly disclaim any) warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this specification, and the entire risk as to implementing this specification is assumed by the implementer. The OpenID Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. The OpenID Foundation invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this specification.

# [Appendix C.](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.appendix.C) [Document History](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#document-history)

[[ To be removed from the final specification ]]

-06

* Incorporated review feeback by Marcos Sanz and Adam Cooper
* Added text on integrity, authenticity, and confidentiality for data passed between OP and RP to Security Considerations section
* added purpose field to claims parameter
* added feature to let the RP explicitly requested certain verification data

-05

* incorporated review feedback by Mike Jones
* Added OIDF Copyright Notices
* Moved Acknowledgements to Appendix A
* Removed RFC 2119 keywords from scope & requirements section and rephrased section
* rephrased introduction
* replaced birth\_name with birth\_family\_name, birth\_given\_name, and birth\_middle\_name
* replaced transaction\_id with txn from RFC 8417
* added references to eIDAS, ISO 3166-1, ISO 3166-3, and ISO 8601-2004
* added note on purpose and locales
* changed file name and document title to include 1.0 version id
* corrected evidence plural
* lots of editorial fixes
* Alignment with OpenID Connect Core wording
* Renamed id to verification\_process
* Renamed verified\_person\_data to verified\_claims

-04

* incorporated review feedback by Marcos Sanz

-03

* enhanced draft to support multiple evidence
* added a JSON Schema for assertions containing the verified\_person\_data Claim
* added more identity document definitions
* added region field to place\_of\_birth Claim
* changed eidas\_loa\_substantial/high to eidas\_ial\_substantial/high
* fixed typos in examples
* uppercased all editorial occurences of the term claims to align with OpenID Connect Core

-02

* added new request parameter purpose
* simplified/reduced number of verification methods
* simplfied identifiers
* added identity\_documents\_supported to metadata section
* improved examples

-01

* fixed some typos
* remove organization element (redundant) (issue 1080)
* allow other Claims about the End-User in the claims sub element (issue 1079)
* changed legal\_context to trust\_framework
* added explanation how the content of the verification element is determined by the trust framework
* added URI-based identifiers for trust\_framework, identity\_document and (verification) method
* added example attestation for notified/regulated eID system
* adopted OP metadata section accordingly
* changed error behavior for max\_age member to alig with OpenID Core
* Added feature to let the RP express requirements for verification data (trust framework, identity documents, verification method)
* Added privacy consideration section and added text on legal basis for data exchange
* Added explanation about regulated and un-regulated eID systems

-00 (WG document)

* turned the proposal into a WG document
* changed name
* added terminology section and reworked introduction
* added several examples (ID Token vs UserInfo, unverified & verified claims, aggregated & distributed claims)
* incorporated text proposal of Marcos Sanz regarding max\_age
* added IANA registration for new error code unable\_to\_meet\_requirement

# [Authors' Addresses](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.authors)

**Torsten Lodderstedt** Lodderstedt yes.com EMail: [torsten@lodderstedt.net](mailto:torsten@lodderstedt.net)

**Daniel Fett** Fett yes.com EMail: [mail@danielfett.de](mailto:mail@danielfett.de)