# Basic Function
## *Attestation of attributes*

# Introduction

This document describes the basic function *Attestation of attributes* in the *TIP-ecosystem*, how existing international/EU standards are applied and what further details and specifications are set within the *TIP-ecosystem*.

As per the definition in *TIP basic functions and definitions*, the *Attestation of attributes* enables *Actors* to identify themselves at a high assurance level by sharing one or more attributes (i.e. properties, characteristics or qualities of an *Actor* (e.g. age, name, diplomas obtained, etc.)). This document specifies the basic function in general, including the particular identity wallet-based architectures as introduced with the European Digital Identity (EUDI) Framework. The EU proposes the so-called European Digital Identity Wallet to promote trusted digital identities for all Europeans allowing *Actors* to be in control of their own online interactions and presence.

This document includes a specification of a desired end state based on international standards currently drafted in the Architecture Reference Framework (ARF)[1] of the EUDI Wallet initiative. With EU certified wallets not being available for wide scale use in the near future, TIP recognizes that domains will follow a growth path towards harmonization. In the meantime TIP basic functions such as *Signing data* and *Exchanging data* can be used for document-based implementations using PDF, XML, XBRL or other file formats. Domain specific implementations can benchmark their implementation on the principles described in this document.

*Actors* in the *TIP-ecosystem* need to identify themselves at assurance level high. *Actors* in the *TIP-ecosystem* can hold a wallet, containing Person Identification Data (PID), (both Natural Person Identification Data (NPID) and Legal Person Identification Data (LPID)) and (Qualified) Electronic Attestations of Attributes (QEAA) that they can share.

The basic function of *Attestation of attributes* in the *TIP-ecosystem* is compliant to the Architecture Reference Framework (ARF) of the EUDI Wallet initiative. Requirements and standards of a wallet solution in the *TIP-ecosystem* are defined below.

Note: This document is published for consultation purposes and can be updated to a 1.0 version after implementation by TIP Partners. This document is written before the WE BUILD pilot and will be updated afterwards when necessary. Comments on this document are appreciated via an email at info@trustedinformationpartners.nl .

[1] The ARF is published to: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/

The functionality is described below in the following chapters



# Description

*Definitions on attestation of attributes*

The definition of attestation of attributes is given in the latest version set in eIDAS2 EU law[2]. For readability purposes the definitions in the regulations are repeated hereafter:

- **Attribute**: a characteristic, quality, right or permission of a natural or legal person or of an object;
- **Electronic attestation of attributes:** an attestation in electronic form that allows the authentication of attributes;
- **Qualified electronic attestation of attributes**: an electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;
- **Authentic source:** a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person and is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice;
- **Person Identification Data (PID):** A set of data enabling the identity of a natural (NPID) or legal person (LPID).

[2] eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN

### *Initialisation of a wallet instance*

A Wallet Provider provides a wallet, which is aligned with the eIDAS2 implementation acts, to the *Actor* which is considered a wallet instance in the operational state when it is installed and activated by the *Actor*. The *TIP-ecosystem* will not require the QTSP to deliver a certified EUDI wallet, but the *TIP-ecosystem* will accept any EUDI certified wallet. For readability purposes the initialisation of a wallet instance according to the ARF is repeated:

- Once a recognised wallet provider has attested the wallet instance, it is considered *operational*.
- Once a recognised PID provider has issued a PID to the operational wallet instance, it is considered a *valid* identity wallet.
- The ARF states that the wallet instance is still *operational* when the PID expires or is revoked. That may affect the validity of an attestation of an attribute or a certificate for QES.
- The *Actor* is able to deactivate its wallet instance.

The ARF tends to focus on natural persons representing themselves. The scope for *TIP* includes *Actors* in general (both natural as legal persons), which poses additional requirements to attestation.

### *Releasing attributes*

The supported standards for releasing attributes are described in the ARF and will be refined, depending on requirements from the use cases (see paragraph Use Cases). TIP expects this to lead to a small subset of standards profiles, one for each type of flow. See the “Preference in TIP” column in the table in the paragraph Standards.

All TSP's (including QTSP's) can provide Non-Qualified Attestations of Attributes as well. A QTSP in TIP has the role of PID Provider as described in paragraph 4.1.3 of the ARF, issuing a PID signed with a qualified certificate.

## Application

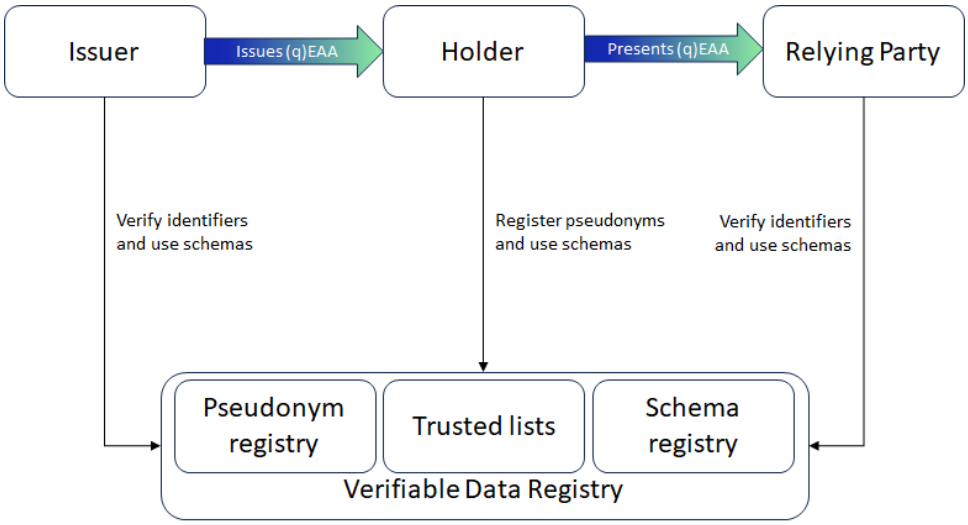
Attributes with Electronic Attestation are issued by the issuer of the attributes to the *Actor* (holder) and are presented by the *Actor* to the verifier/relying party .

A *TIP* compliant *Acting space* is required to support this exchange of attestations. The following transitions of attributes are possible:

1. An *Actor* retrieving an attribute from an issuer.
   Alternatively, an interaction pattern exists where an issuer pushes an attribute.
2. An *Actor* releasing (presenting) the attribute to the relying party / verifier.
   Multiple release patterns are possible, these are described below.
3. Revoking an attribute by an issuer of an attribute.

Based on these transitions, the attribute can be valid, expired or revoked.

*Release patterns*




Multiple release patterns for the presentation of attributes are possible. Two are described here.

1. An interactive release of attributes where the *Actor* is in the loop during the transaction and authorizes it on the spot. This exchange pattern is described in detail in the ARF, as the "proximity (un)supervised flow" and the "remote cross-device/same-device" flow. In interactive release, the relying party generates an authentication challenge and the *Actor* responds with a presentation cryptographically linked to that challenge.
2. A non-interactive release of attributes where the *Actor* selects and consents for one or more attributes for sharing with a relying party at a later moment in time. The attributes are available for sharing with/collection by the relying party in the *Actor*'s *Acting space*, which ensures that sharing only takes place within the parameters of the *Actor*'s predefined consent. It is the responsibility of the *Acting space* to interactively authenticate the attributes and to enforce an authorisation policy based on the *Actor*'s consent.

*Intended outcome*

Attestations can have the following capabilities:

- *Compound proof*: a combination of attestations can prove more about the Actor (in the form of verifiable presentation).
- *Selective disclosure*: the capability that enables the Actor to present a subset of attributes provided. For example, don't disclose your income, but disclose only the proof you earn more than a certain amount. ARF requires support of selective disclosure (see the paragraph Standards below).

As stated in the ARF Outline, selective disclosure and combination of attestations can be handled in two different ways:

1. The wallet has a broad collection of attributes, each time a specific attribute is required, a new attestation has to be requested from providers.

2. The wallet has the intrinsic capability to selectively disclose or derivate a specific attribute and aggregate attributes without the need for new attestations or interactions with Issuers (specific fit for purpose signature schemes could enable this).

## Agreements

Actors can authenticate themselves with an eIDAS2 compliant authentication provider (such as DigiD, eHerkenning). Attributes can be created from the PID data retrieved from this authentication provider.
TIP defines the minimal set of attributes that are needed to identify the Actor as described by eIDAS.

**TIP quality criteria on interim wallet solutions until EUDI wallets are commonly available**

- Users have been identified with level of assurance High during the initialisation of the wallet. While the wallet is valid, the *Actor* can use the PID data for identification with assurance level High. Users have access to their A*cting Space* with an authentication mechanism that can resist attacks with a high attack potential as mentioned in the eIDAS regulation 2015 1502.
- Attributes can only be shared with consent of the *Actor*. There are guarantees in place that users give consent for presenting attributes.
- The origin and authenticity of qualified attributes are beyond question. The mechanism used to proof the origin and authenticity is a qualified digital seal or signature by the issuer (the owner of the authentic source). The same mechanism is used for attributes or statements given by the user self. The user can issue a statement/attribute and sign it with his/her own qualified digital signature.
- Interim solutions safely store the user's attributes, guaranteeing their availability and authorized access only.
- Interim solutions guarantee that the request for attributes of relying parties (which should be signed) are stored and available for the user. This can be used as evidence when legal challenges occur.

## Standards

The following components have been identified as relevant for the attestation of attributes in the *TIP-ecosystem*:

- **Cryptographic keys management system.** This component is responsible to manage and store cryptographic information like the private keys generated for instance during the PID issuance process.
- **Attestation exchange Protocol**: This protocol defines how to request and present the PID and the Attestation of Attributes in a secure and privacy preserving fashion. The protocol also defines how authentication is performed with the Relying Party.
    - OpenID for Verifiable Credentials
- **Issuance Protocol**: This protocol defines how PID and Attestation of Attributes should be issued and in which formats.

    - OpenID for Verifiable Presentations
- **Data model**: the data model defines and describes the data elements and how they interact with each other and their properties
  Possible standards:
    - mDL
    - Verifiable Credentials
- **PID and (Qualified) Electronic Attestation Attributes schemas**: The attestation schema contains the structure and the logical organisation of the data that defines the properties of the attestation. The attestation schema also contains additional information including, but not limited to, the verification mechanisms and the underlying identity assurance to which the properties are related, and the proof of possession by the *Actor*
- **PID and (Qualified) Electronic Attestation of Attributes formats**: Those formats are used to represent the characteristic, quality, right or permission of the actor in the form of signed and verifiable digital artefacts. See table below.
- **Signature formats**: Technical implementation of one or more mathematical methods in the form of a digital artefact, aimed at demonstrating the authenticity of a digital document, its integrity, authenticating the author of a document and optionally also its recipient (audience of the document).
- **Trust model**: collection of rules that ensure the legitimacy of the entities involved:
    - User/Actor authentication
    - Issuers identification / registration
    - Recognised data models and schemas
    - Relying parties' registration and authentication
- **Cryptographic suites and mechanisms**: Algorithms and methods that secure the data exchange in terms of confidentiality and integrity.
- **Validity status check**: Mechanism to publish and obtain information about validity status of, inter alia, PID, (Q)EAA, certificate, etc.

The ARF makes a distinction between a type 1 and type 2 wallet configuration.
Type 1 configuration is aimed at use cases where the Relying Party relies on guarantees for the Level of Assurance (LoA) as defined in CIR 2015/1502, enabling cross border identification. EUDI Wallet solutions MUST support Type 1 configuration that is mandatory for PID.
Type 2 configuration aims to enable flexibility and additional feature support for (Q)EAA use cases that cannot be met by Type 1 configuration (e.g. for additional privacy or adoption reasons).

For the issuance of attributes, the attributes must adhere to the requirements as described in paragraph 5.2.1 *Issuing requirements for (Q)EAA* of the ARF.
However, TIP can allow more standards to support what is usable and is used in current *Information chains*.

## Best practices

For the *TIP-ecosystem* the following best practices are recommended.

1. It is recommended for an EUDI Wallet to show the current status of a credential (e.g. issued, valid, expired or revoked). This is not a requirement by the ARF but is customer friendly towards the *Actor*.

2. It is recommended for an EUDI Wallet to periodically check whether the credential is revoked. This allows an *Actor* to sort out the reason for revocation with the issuer ahead of engaging in a transaction and finding out the credential is revoked during the transaction. This recommendation does not replace the requirement for Relying Parties to validate attestations and certificates upon acceptance, including checking for expiration and revocation.

## Use cases

The following table gives an overview of examples of use cases relevant for the attestation of attributes:

| Use case | Used attributes | Issuer | Verifier | Holder |
|---|---|---|---|---|
| Mortgage lending (“Hypotheekverstrekking”)<br><br>Financial advisor as authorized person. | 1. Income statement<br>2. Employer declaration (“werkgeversverklaring")<br>3. Arbeidsverleden<br>4. Geregistreerde leningen<br>5. Studieleningen bij DUO<br>6. Verklaring van vermogen<br>7. Burgerlijke staat<br>8. Informatie over garantsteller | Tax office<br>UWV<br>Employer<br>BKR<br>BRP<br>DUO | Mortgage Lender | Home owner |
| Hiring an employee (“Indiensttreding”) | 1. VOG<br>2. Diploma<br>3. Declaration of qualification of profession<br>4. Driving licences, boating license, pilot's license<br>5. Certificates such as VCA, BHV<br>6. Company data (for secondment)<br>7. Role and mandates within employer organization | Justis, DUO, NBA, BIG, RDW, employer | Employer | Employee |
| Authorizing accountant for tax actions.<br>(“Autoriseren voor fiscale handelingen”) | 1. Mandate from customer<br>2. Mandate from accountant office | Customer<br>Accountant office | | |
| Pre-filled declaration (“Vooringevulde Aangifte”)<br><br>Data from tax office, subset of data signed by third party. | 1. | Tax Office | | Accountant |

## Supplier(s)

EUDI Wallets are to be provided by EUDI Wallet Providers. These providers need to comply with ARF guidelines and adhere to national laws and regulations. The exact procedure is yet to be drafted at moment of writing. There is no requirement for EUDI Wallet Providers to be a QTSP. However, QTSP's are likely to become wallet providers since their organization and technology is already geared towards adherence to similar national laws and regulations.
In the ARF a distinction is made between Person Identification Data (PID) and (Qualified) Electronic Attestations of Attributes (Q)EAA. The PID data requires a digital identity as source, meaning a QTSP is to be involved at some point to initialise the EUDI Wallet using PID data, including verification at set intervals for the wallet to remain active.

## Administrator(s)

The basic function *Attestation of attributes* does not require central management from *TIP-ecosystem*. The functionality is provided by *Acting spaces* and *Value-added service* providers (wallet providers).

## Regulator(s)

EUDI Wallet Providers are expected to provide access to their services in accordance with European and national laws and regulations. Detailed terms of engagement between each provider and the *Actor* must be defined clearly before any service is rendered – this agreement will reflect how funds exchange happens, fees for using wallets or *Value-added services*, dispute resolution mechanisms, liability provisions etc.

## Costs

If *Attestation of attributes* is not carried out (for free) from European Digital Identity Wallets, prices for the use of the basic function *Attestation of attributes* are established on the basis of bilateral agreements between *Issuers, Relying parties* and *Actors* who use these via *Acting spaces*. Payment is made through the basic function *Making payments*.
Possibly the issuers of attributes may charge a fee for their services. This is also the case present day where fees are charged for certain attestations on paper.

# Annex

TIP follows the requirements as described in the ARF or has a subselection based on the use cases TIP wants to support. The preference for a specific protocol/standard is described in the "Preference in TIP" column. For some components no preference is given yet. We would like to gain feedback from our community on the preferences on these components.

| Component | Requirement | Preference in TIP |
|---|---|---|
| Cryptographic Keys Management System | One of the following components MUST be supported:<br>1. Embedded Secure Element or Trusted Execution Environment<br>2. External device (Secure Elements / Smart Cards)<br>3. Backend (remote HSM) | Does TIP have a preference for a Keys Management System? |
| Attestation Exchange Protocol - 1 | Support OpenID4VP for attestation exchange for remote flows.<br>Request parameters should be in accordance with OpenID SIOPv2 | For some chains, support of asynchronous exchange is required. Is this possible with OpenID4VP? |
| Attestation Exchange Protocol - 2 | Support the protocol detailed in the standard ISO/IEC 18013-5:2021 for proximity flows | |
| Attestation Exchange Protocol -6/7 | [..] support Selective Disclosure of attributes as specified in ISO/IEC 18013-5:2021 and SD-JWT | Preference for ISO/IEC 18013-5:2021 or SD-JWT? |
| Issuance Protocol - 1 | Support OpenID4VCI as an issuance protocol. | |
| Data Model -1/2 | Support attestations in accordance with the data model specified in ISO/IEC 18013-5:2021 (mDL) or W3C Verifiable Credentials Data Model 1.1 | Preference for ISO/IEC 18013-5:2021 (mDL) or W3C Verifiable Credentials Data Model 1.1? |
| PID Attestation Formats-1/2/3 | Support attestation in JWT and SD-JWT format / CBOR format / JSON-LD format | |
| Cryptographic suites and mechanisms -1 | Support cryptographic suites and mechanisms used for attributes detailed SOG-IS Agreed Cryptographic Mechanisms Version 1.2 | Use what a government body requires in a specific chain. |

| | | |
|---|---|---|
| | | Basis for cryptographic suites is what the Dutch government (Logius) or NIST accepts regarding encryption /signing / hashing algorithms, such as:<br>• Agreed Assymetric Encryption Scheme<br>• Agreed Digital Signature Scheme)<br>To be defined in Security Standards and Regulations) |

## Sources

| Link | Description | Author/Source |
|---|---|---|
| EBSI Verifiable Credentials Playbook - EBSI Specifications | EBSI Verifiable Credentials Paybook | EBSI |
| The European Digital Identity Wallet Architecture and Reference Framework | Set of the specifications to develop an interoperable European Digital Identity (EUDI) Wallet Solution | EDI / europa.eu |
| Releases - EUDI Documentation (Github) | Set of the specifications to develop an interoperable European Digital Identity (EUDI) Wallet Solution in Github | EDI / Github |
| Outline - European Digital Identity Architecture and Reference Framework | Summary description of the eIDAS expert group's understanding of the EUDI Wallet concept. | EDI |

List of observations to be evaluated in next version

| Nr | Title | Remarks |
|---|---|---|
| **01** | Revocation methods | Possible options (to be discussed)<br>- Revocation lists (Bitsring Status list v1.0)<br>- Short time to live for mDOC/mDL (ISO/IEC 18013<br>- Non-revocable |
| **02** | | |
| **03** | | |
| **04** | | |
| **05** | | |
| **06** | | |
| **07** | | |