IBAN Attestation Data Rulebook

1. Introduction

Disclaimer: This document is a draft in the context of IBAN attestation for individuals. A version of the IBAN Attestation Rule book for businesses is available/in draft state. This document builds on that to support IBAN attestation for individuals. Eventually perhaps both these rulebooks can be merged into a single rulebook. Also, this document uses the term (Q)EAA to cover both EAA and QEAA. At a later time, the document will be updated to refer to either 'EAA' or 'QEAA'.

1.1 Scope

This document serves as the International Bank Account Number (IBAN) Attestation Rulebook for issuing IBAN attestations to individuals' EUDI wallets. It outlines the requirements specific to IBAN attestation, including the processes for its issuance and verification. The rulebook provides information on the background and attributes of IBAN attestation, its trust infrastructure, and technical implementation.

The IBAN attestation is intended exclusively for use by natural persons (individuals).

Topic 10/23 in the ARF 2.2 specifies that attestation must be issued in the [SD-JWT VC] format, among others. This rulebook is designed to align with the [SD-JWT VC] requirements.

1.2 Background

The necessity for IBAN attestation stems from the extensive use of IBANs for cross-border banking and payment transactions within the SEPA (Single Euro Payments Area) and beyond. Financial institutions and service providers require a secure, standardized method to verify bank account ownership to mitigate fraud, enhance trust, and improve process efficiency.

1.3 Goal of the IBAN attestation

The IBAN attestation is designed to: Provide a secure and verifiable credential to confirm a natural person's ownership of an IBAN.

1.4 Key words

This document uses the capitalized key words 'SHALL', 'SHOULD', and 'MAY' as specified in [RFC 2119], i.e., to indicate requirements, recommendations, and options specified in this document.

Additionally, 'must' (non-capitalized) is used to denote external constraints mandated by other documents or regulations. The term 'can' indicates capability, while terms like 'will,' 'is,' or 'are' are used as factual statements.

1.5 Terminology

The terminology in this document follows Regulation (EU) 2024/1183.

To fully understand the data schema, the following definitions are provided:

- **IBAN** (International Bank Account Number): A standardized international numbering system used to uniquely identify a bank account. The format includes a two-letter country code, check digits, and a basic bank account number (BBAN).
- **IBAN Attributes:** Attributes related to an IBAN to be stored along with the IBAN in the IBAN attestation.
- **BBAN:** Basic Bank Account Number. An IBAN consists of a two-letter country code, two check digits and a Basic Bank Account Number. A BBAN includes information about the domestic bank and account number.
- **Account Token:** Account tokens are functional tokens surrogate for the IBAN and is specific to Device and Wallet. Account tokens carry benefits related to traceability and control and lifecycle management.
- **Holder**: A legal person who owns the bank account associated with the IBAN.
- **ASPSP** (Account Servicing Payment Service Provider): A financial institution that provides and maintains payment accounts accessible via online platforms.
- **PSD2** (Payment Services Directive 2): An EU directive that regulates payment services and providers throughout the European Economic Area, promoting competition and innovation.
- **SCA** (Strong Customer Authentication): A requirement that ensures electronic payments are performed with multi-factor authentication to increase the security of electronic payments. It is a requirement of the PSD2 on payment service providers.

- **BIC** (Bank Identifier Code): A unique code assigned to financial institutions used to identify the bank during international transactions. Also known as the SWIFT code.
- **Clearing Number**: A number used to identify a financial institution or a branch within a country's clearing system.
- **SWIFT** (Society for Worldwide Interbank Financial Telecommunication): A global provider of secure messaging services and financial transactions among banks and financial institutions.
- **Open Banking**: The practice of enabling third-party financial service providers to access banking and transaction data via APIs, typically under PSD2 compliance.

2. IBAN Attestation Issuance process

Financial institutions acting as Account Servicing Payment Service Providers (ASPSP) or entities authorized to act on behalf of a financial institution are authorized to issue IBAN attestations. These entities are considered the authentic sources of IBAN information. Issuance may occur directly or through a delegated (Qualified) Electronic Attestation Authority ((Q)EAA).

The issuance process must comply with relevant EU regulatory and technical standards, including PSD2, to ensure secure and standardized account information access.

In the EWC context, a generic attestation issuance process, as described by wallet providers in the pilots, is outlined in RFC-001.

Only individuals possessing a valid PID in their wallets can request IBAN attestations. Consequently, these attestations can only be issued to EUDI-compliant individual wallets.

During the issuance process, it is important to establish that the wallet holder is the same person as the account holder. During the communication with the bank authorization server it is important to perform step-up authentication, and this process might also involve the wallet to present the PID during this authentication. Only after this is complete will the OAuth 2.0 access token be issued that is required to request the IBAN credential. If the credential API will be offered by the (Q)EAA, the (Q)EAA needs to have a way to verify the access token. This can either be via a real-time call, or if possible, the bank and (Q)EAA may have agreed to pre-share some cryptographic keys to allow the (Q)EAA to verify the access token directly without real-time consultation of the bank.

3. IBAN Attestation Verification process

In the EWC context, wallet providers have described a generic verification process during the pilots, outlined in RFC-002.

Optionally, during the presentation of the IBAN attestation, account tokens can be validated by the attestation provider.

4. IBAN Attestation attributes

This table contains the name of the attribute, its description, and whether the attribute is required or not.

Property Name	Description	Required
bank_account	Attributes representing the bank account.	Yes
account_name	Name of the account, generated by the bank or customized by the owner.	Yes
IBAN	International Bank Account Number, as defined in ISO 13616:2020.	Yes
account_type	Nature of the bank account.	Yes
account_currency	Currency code used of the account, as defined in ISO 4217:2015.	Yes
account_usage	Specification about the private or professional usage of the account. This additional information allows to further distinguish personal bank accounts from professional bank accounts.	No
bank_account_token	Attributes representing the bank account token	No
account_token_number	International Bank Account Number, as defined in ISO 13616:2020. Surrogate for IBAN, can be device- and wallet specific.	Yes
masked_account_number	The masked account number to which the bank account token is linked.	Yes
token_attributes	JSON formatted list of token attributes and values	No

Property Name	Description	Required
account_ownership	Attributes representing the account ownership.	Yes
owner_name	Legal name of the legal person owning the account.	Yes
parties	List of parties involved in the account ownership.	No
full_name	Full name of the physical person.	Yes
role	Role of the physical person.	Yes
account_provider	Attributes representing the account provider.	Yes
provider_name	Name of the financial institution providing the account.	Yes
bank_identifier	Bank identification number.	Yes
provider_country	Alpha-2 country code, as defined in ISO 3166-1, of the provider country or territory.	Yes
BIC	BIC or SWIFT code, as defined in ISO 9362, of the financial institution.	No
clearing_number	Clearing number, only used in some countries, of the identification of the financial institution.	No

IBAN Attestation metadata are aligned with the metadata of organizational credential attestations already defined in EUDI wallet data schemas

This table contains the name of the metadatum, its description, and whether the metadatum is required or not.

Metadatum Name	Description	Required
issuing_authority	Attributes representing the bank account.	Yes
issuing_authority_id	Name of the account, generated by the bank or customized by the owner.	Yes
issuance_date	International Bank Account Number, as defined in ISO 13616:2020.	Yes
expiry_date	Nature of the bank account.	Yes
authentic_source_id	Currency code used of the account, as defined in ISO 4217:2015.	Yes
authentic_source_name	Specification about the private or professional usage of the account.	No
credentialSubject	Attributes representing the account ownership.	Yes

The IBAN Attestation schema is available in the EWC schemas and rulebooks repository: IBAN data schema.

4.1 Minimum number of optional IBAN attestation attributes

There is no minimum number of optional attributes for the IBAN. Each Issuer will have the responsibility to fill in the attributes when provided by the original source.

5. Trust infrastructure details

In this chapter, trust requirements and general considerations regarding the IBAN attestation itself are described.

5.1 Trust requirements on the IBAN Attestation

In the ARF 2.2, the following information for (Q)EAAs Providers is given.

(Q)EAAs Providers are trusted entities responsible to:

- Verify the identity of the EUDI Wallet User in compliance with LoA high requirements.
- Issue attestations to the EUDI Wallet in a harmonized common format.
- Make available information for Relying Parties to verify the validity of the attestation.

The IBAN Attestation SHALL contain the electronic signature or the electronic seal of the issuing body and adhere to the legal requirements defined in Annex VII of the Regulation (EU) 2024/1183.

The IBAN Attestation SHALL follow the SD-JWT format.

IBAN Attestation Issuers SHALL follow the IBAN requirements and trust mechanisms defined by Authentic Sources on a national level. Common legal trust mechanisms need to be established for the trust ecosystem to be trustworthy:

- The IBAN SHALL be unique and agreed upon on EU and EES level.
- There SHALL be one common schema for the IBAN Attestation.
- The IBAN SHALL be in the format as described in in ISO 13616:2020.
- The IBAN SHALL apply for all natural persons.
- The issuer of the IBAN SHALL be responsible for its revocation.

5.2 Trust a signature or seal over an IBAN

To trust a signature or seal over an IBAN, the Relying Party needs a mechanism to validate that the public key it uses to verify that signature or seal is trusted. OpenID4VP provides such mechanisms. However, additional details need to be analyzed to fully specify these mechanisms for IBANs within the EUDI Wallet ecosystem and the trust anchor for it. It is assumed that this will be part of a detailed specification from a standardization authority.

5.3 IBAN Provider Trusted List

For authenticating IBANs, trust anchors will be used that are present in an IBAN Issuer Provider Trusted List.

5.4 SD-JWT-compliant

IBAN is fully compliant with [OpenID4VP] and [SD-JWT VC].

6. References

- RFC-001: Issue Verifiable Credential
- RFC-002: Present Verifiable Credentials

- SD-JWT VC: SD-JWT VC Specification
- OpenID4VP: OpenID4VP Specification