Abstract

An Internet IBAN (IIBAN) identifies an internet-based financial endpoint in a manner that is superset-compatible with the existing European Committee for Banking Standards (ECBS) International Bank Account Number (IBAN) standard [ISO13616].

Status of this Memo

This memo defines an Experimental Protocol for the Internet community. This memo does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This document is an individual submission. Comments are solicited and should be addressed to the author(s).

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on May 16, 2012.
1. Introduction

An Internet IBAN (IIBAN) identifies an internet-based financial endpoint. No assumptions are made about settlement paths, currencies or commodities being exchanged, or trust relationships between parties. IBAN provides a building block with which the internet community can develop viable, interoperable alternatives to legacy financial systems.

Technically, IIBAN is an unofficial superset of the European Committee for Banking Standards (ECBS) International Bank Account Number (IBAN) standard [ISO13616] that is increasingly used in conventional global financial networks, including outside of its original home of Europe. Against the IBAN registry [IBAN-REG], IIBAN subsumes the position of National Numbering Authority (NNA) for the nominal [ISO3166] ‘nation’ of AA (the Internet) in order to provide a financial endpoint registrar service for the internet community.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].
Table of Contents

1. Introduction ........................................ 2
2. Requirement........................................... 4
3. Solution............................................... 4
   3.1. ISO13616 (IBAN).................................... 4
   3.2. IIBAN.............................................. 5
4. General Considerations.............................. 7
   4.1. Issues of Centralization......................... 7
   4.2. Country Code..................................... 8
   4.3. Institution Identifiers........................... 8
      4.3.1. Issuing Paradigms............................... 8
         4.3.1.1. Proxied Issue Schemes................... 8
         4.3.1.2. Distributed Hash Table (DHT) Schemes ........ 9
         4.3.1.3. Private Issue Schemes.................... 10
         4.3.1.4. IIBAN’s Combined Issue Scheme............ 10
      4.3.2. Why Institutions?............................. 11
      4.3.3. Number of Institutions....................... 11
      4.3.4. Number of Endpoints per Institution........... 11
      4.3.5. Intra-Institution Routing...................... 12
   4.4. BBAN Length..................................... 12
5. Implementation Considerations...................... 13
6. Security Considerations............................ 13
   6.1. Non-Linear Issue................................ 13
   6.2. Validation....................................... 13
   6.3. IANA Processes................................... 13
7. IANA Considerations.................................. 14
   7.1. Institution Identifiers......................... 14
      7.1.1. Name Space Exhaustion....................... 14
      7.1.2. Registration.................................. 14
      7.1.3. Modification / Cancellation................... 14
      7.1.4. Expiry........................................ 15
   7.2. Publications.................................... 15
      7.2.1. IIBAN Institution Identifier Registry.... 15
   7.3. ISO Liaison...................................... 15
   7.4. Security......................................... 15
8. References............................................ 16
   8.1. Normative References............................. 16
   8.2. Informative References......................... 17
9. Contributors.......................................... 18
10. Acknowledgments..................................... 18
11. Authors’ Addresses.................................. 18
2. Requirement

In recent years the internet has seen the emergence of an increasing variety of online financial settlement scenarios. Such scenarios include web based commerce, high frequency trading (HFT) on stock markets, mobile phone ‘in app’ payments, mobile near field communication (NFC) physical proximity-based payments, online banking based bill payment, and interpersonal payments within Massive Multiplayer Online Roleplaying Games (MMORPGs) amongst others. These scenarios vary in at least the following aspects:

* Typical payment size
* Acceptable settlement latency
* Currencies or commodities supported
* Nature of trust relationships between parties (if any)
* Requirement for offline operations

Despite these differences, in each case the need remains to precisely identify each of the parties within a transaction.

Given this trend, it makes sense to propose a standard mechanism for the consistent, global identification of internet-based financial endpoints. IIBAN provides such a mechanism.

3. Solution

3.1. ISO13616 (IBAN)

For inspiration we look toward emerging standards for international financial endpoint identification in conventional financial networks. Today’s most widely widely adopted international standard in this area is the European Committee for Banking Standards (ECBS)’ IBAN [ISO13616], which builds upon the ISO’s 2-character country identification scheme [ISO3166].

The format of an IBAN is as follows:

<ISO3166-1 alpha2 country> + <2 digit checksum> + <BBAN>
The checksum is calculated as follows:

1. Set the checksum digits to ‘00’.
2. Re-arrange the string such that the BBAN comes first, then the country code, and finally the ‘00’ or blank checksum.
3. Transpose the letters A-Z to the numbers 10-35, expanding the string as appropriate.
4. Convert the string to an integer, ignoring leading zeros.
6. Subtract the checksum from 98 and, if necessary, pad with a leading 0 to make a two digit number.

The BBAN is a nation-specific ‘Basic Bank Account Number’ that must be fixed length for any given nation but whose length may vary between nations. National formats are specified by National Numbering Authorities (NNAs). SWIFT’s IBAN registry [IBAN-REG] aggregates each national scheme into the global IBAN standard.

3.2. IIBAN

In order to issue financial endpoint identifiers within the IBAN [ISO13616] scheme IANA assumes National Numbering Authority (NNA) or ‘nation’ status for the nominal nation of ‘AA’ (the Internet).

The IIBAN format may be expressed in ABNF [RFC5234] as follows:

```
iiban = "AA" checksum bban          ; eg: AA12011123Z56
checksum = 2digit                      ; eg: 12
bban   = institution account         ; eg: BNK123Z56
institution = rsv-inst / std-inst     ; eg: 010 or BNK
rsv-inst = "0" 2char                   ; eg: 010
std-inst = nonzerochar 2char           ; eg: BNK
account = 6char                       ; eg: 123Z56

char = digit / letter
digit = "0" / "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"
```

Walter Stanish. Payward Inc. Section 3.2. [Page 5]
An explanation of the major elements follows.

iiban:
A structurally valid IIBAN.

checksum:
Two checksum digits as per the IBAN standard, the algorithm for which is described above. These digits are used to detect transposition errors, preventing accidental misrouting.

bban:
The Basic Bank Account Number (BBAN) is the portion of an IBAN defined by a National Numbering Authority (NNA). In our nominal nation of ‘AA’ (the Internet), the BBAN defines the structure of an internet-based financial endpoint as being comprised of a three character institution code followed by a six character institution-specific endpoint identifier.

institution:
The three character institution code identifies either a reserved portion of the name space or a registrant of institution status. Three characters provides for a total of 46,656 institution codes (36^3). Reserved institution codes are those that begin with zero (‘0’), whilst all other codes are available for IANA to assign to registrants.

The following table defines reserved institution codes and the approximate number of codepoints within their name space.

<table>
<thead>
<tr>
<th>Code</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>000-009</td>
<td>(Reserved for future use)</td>
</tr>
<tr>
<td>010</td>
<td>Private Use (ala IPv4 10.x.x.x [RFC1918])</td>
</tr>
<tr>
<td>011</td>
<td>Documentation, public works of fiction</td>
</tr>
<tr>
<td>012-0ZZ</td>
<td>(Reserved for future use)</td>
</tr>
</tbody>
</table>

account:
A six character, institution-specific, institution-assigned endpoint identifier. The identifier length allows for 2,176,782,336 endpoints (36^6) per institution.
4. General Considerations

4.1. Issues of Centralization

Conventional financial settlement systems typically assign endpoint creation, maintenance, and identification responsibility to large incumbent players (for example banks, major telecommunications carriers, online payment processors, credit card companies, stock exchanges or brokerage firms). In addition, financial settlement processes themselves typically occur via a relatively small number of relatively centralized networks.

Whilst this centralized approach is understandable from an historic perspective, today its age and drawbacks are becoming more visible.

* Systems integration and maintenance overheads due to disparate endpoint identification schemes, centralized endpoint identifier validation and differing prerequisite communications security configurations (for example, TLS client certificates [RFC5246])

* Poor fault tolerance. Incumbent players and their physical, legal and communications infrastructure represent undesirable Single Points of Failure (SPOFs) that act to reduce system availability. Classic examples of this are banking services that suspend over the weekend, and unpredictable international settlement delays due to differing holidays affecting financial services in foreign jurisdictions.

* Potential for abuse. Attackers (or indeed individual nation-states or organizations within conventional centralized financial systems) may consider temptation for abuse too great to resist. Abuses observed include constant, passive, warrantless surveillance of entire populations [SWIFT2], illegal financial blockade [WL] [WL2] and abusive asset seizure [WSJ].

It is hoped that IIBAN will assist the internet community to develop systems that move beyond the above limitations.
4.2. Country Code

In order to issue bank account numbers within the IBAN [ISO13616] scheme, National Numbering Authority (NNA) or ‘nation’ status must be assumed. An appropriate [ISO3166] two letter country code must therefore be selected, ideally one that is not either in formal issue by the ISO or used informally by various global bodies.

One such code is ‘AA’. This code is considered particularly attractive for the following reasons:

* It is unlikely that a country will emerge that is best identified with ‘AA’. The ISO appears to recognize this fact, since in ISO 3166-1 [ISO3166] ‘AA’ is specified in the series of elements for user purposes which the ISO 3166/MA will never issue.

"If users need code elements to represent country names not included in this part of ISO 3166, the series of letters AA, QM to QZ, XA to XZ, and ZZ, and the series AAA to AAZ, QMA to QZZ, XAA to XZZ, and ZZA to ZZZ respectively and the series of numbers 900 to 999 are available."


* 'AA' will appear above legacy, centralized financial systems in alphabetically sorted destination lists

* Users from international locations in which Roman letters are not frequently used are more likely to recognize ‘AA’ as two of the first letter of the Roman alphabet than arbitrary alternatives

* The letter ‘A’ tends to have positive connotations

IIBAN therefore employs ‘AA’ as a virtual [ISO3166] two letter country code to represent the Internet.

4.3. Institution Identifiers

4.3.1. Issuing Paradigms

4.3.1.1. Proxied Issue Schemes

Conventional financial systems generally require a facilitating institution to issue financial endpoint identifiers on behalf of
participants; for example, banks might issue account numbers on behalf of individuals or businesses. Such de-facto identifier issuing paradigms can be described as 'proxied' in that it requires participants to approach the network via one of a number of mediators in order to obtain a viable financial endpoint.

Drawbacks to this approach include:

* Inefficient name space utilization. Individual institutions are unlikely to achieve complete utilization of endpoint identifiers within their delegated name space.

* Issues of centralized financial systems, described above.

The benefits of this approach are:

* Facilitates effective name space delegation to financial institutions who might apply differing models or guidelines to endpoint identifier issue, therefore encouraging heterogeneity.

* Already an operational and widely understood/accepted model within conventional financial service industries.

4.3.1.2. Distributed Hash Table (DHT) Schemes

Using distributed hash tables (DHT) or a similar mechanism it may be possible to provide dynamic identifier name space management within a financial network itself, such that individual users can self-issue IIBANs and have them corroborated by other network participants.

Drawbacks to this approach include:

* The ‘always on, always connected’ requirement of most of these architectures.

* The ‘endpoint exposure’ problem. IP addresses for critical financial systems are generally made available to a DHT network, which MAY not be desirable in a financial services setting.

* Name space exhaustion. Without some underlying capability for reliable network participant identification, a single party could request vast quantities of identifiers in a bid to disrupt the network through name space exhaustion or processing overhead, causing Denial of
Service (DoS).

The primary benefit of this approach is that it is completely decentralized, thus avoiding the issues associated with centralization (described above).

4.3.1.3. Private Issue Schemes

Just as the Internet Protocol provides a mechanism for Address Allocation for Private Internets [RFC1918], so too IIBAN provides a mechanism for address allocation for private financial networks. Private financial networks might include those operated in Massive Multiplayer Online Roleplaying Games (MMORPGs), financial simulations, technical documentation or fictional works of media.

The reserved institution code ‘010’ is normally used for such purposes.

However, just as the latter two use cases (documentation and media) are segregated from the normal name space in standards for both telephony [NANPA, OFCOM] and IPv4 addressing [RFC5737], IIBAN also maintains a segregated address space (under the ‘011’ reserved institution code) for this subset of private issue purposes.

4.3.1.4. IIBAN’s Combined Issue Scheme

The benefits and drawbacks of various issuing paradigms have already been discussed. IIBAN’s combined issue paradigm allows the balancing of these against other requirements, such as IANA’s need to perform name space management. Under this scheme, proxied issue is facilitated through IANA managed institution registration, provision for two types of privately issued addresses is reserved within this document, and registered institutions COULD provide DHT or similar mechanisms for the management of their delegated name space. The combined issue paradigm offers adequate provision for both manageability and decentralization, whilst maintaining heterogeneity.
4.3.2. Why Institutions?

With the advent of decentralized virtual currencies such as [BITCOIN] the conventional idea of a financial institution (such as a bank) may be seen by some as somewhat superfluous. However, the notion remains useful:

* Conventional currencies will not disappear in the conceivable future, so the notion of financial institutions is expected to endure at least as providers of currency exchange and holding services.

* Systems such as [BITCOIN] have quirks that require slightly delayed settlement due to the nature of their decentralized, consensus-based approach to fiscal transfer. Users requiring instant settlement MAY thus see benefit in the use of a centralized proxy system or organization as an instantaneous financial settlement provider (the ‘institution’).

* IANA MAY delegate management of portions of the IIBAN name space through such institutions.

4.3.3. Number of Institutions

The current global SWIFT BIC [ISO9362] system used for international inter-institution transaction addressing is reported to possess over 7,500 ‘live’ codes, and an additional 10,000 codes that may be used for manual transactions. We therefore assume a requirement to support at least 15-20,000 institution identifiers within the IIBAN system. More than double this number has been provided for.

4.3.4. Number of Endpoints per Institution

With the exception of India and China, the largest nations’ populations are all well below 1 billion. We provide over two billion endpoints per institution, which should be more than adequate.
4.3.5. Intra-Institution Routing

In reference to routing identifiers used in most conventional financial networks (such as ‘sort code’ or ‘branch code’), intra-institution routing identifiers have been purposefully excluded from IIBAN.

Institutions MAY create their own address space segmentation schemes in the event that they wish to divide financial endpoints between disparate physical or logical systems, however it is observed that this relic of an earlier financial era of disconnected systems will probably be gradually phased out over time - at least as a public-facing identifier.

4.4. BBAN Length

BBAN lengths in the official registry [IBAN-REG] seem to be determined solely by National Numbering Authorities (NNAs) and appear to have no specific length limitation. In practice, however, they vary between about 11 and 26 characters. To avoid issues of backwards compatibility with existing systems, exceeding this limit is undesirable.

Existing NNAs seem to determine BBAN formats simply by concatenating existing national account identifiers such as institution, branch and account number. Because these numbers are typically very old they are often longer than strictly required because legacy identifiers:

* Are sometimes numeric only (ie: do not include letters), or a significant portion of the BBAN is numeric only.

* Often include secondary checksums that were instituted to avoid financial endpoint transposition errors in the days prior to electronic banking. Such secondary checksums are no longer required for non-legacy transactions due to IBAN’s built-in checksum feature.

Thus by allowing alphanumeric values for each character and relying solely upon IBAN’s checksum, IIBAN increases the effective capacity of an identifier without increasing its length.
5. Implementation Considerations

Implementers SHOULD aim to accept both IIBAN and IBAN equally in all cases, such that end users are NOT aware of any difference between the standards.

6. Security Considerations

IIBAN only provides an endpoint identification scheme and DOES NOT approach problems of communications security, which are purposefully left to other protocols. Even so, some security considerations are pertinent.

6.1. Non-Linear Issue

To preserve the anonymity of clients and to refrain from leaking information about the number of financial endpoints created over a given period, institutions SHOULD refrain from issuing IIBAN in a sequential manner. Instead, a random or semi-random sequence of issue SHOULD be adopted.

6.2. Validation

IBAN [ISO13616] and, by extension, IIBAN provide checksum digits for algorithmic identifier validation. Implementers MUST be aware that the checksum is intended primarily for the early detection of transposition errors. An IIBAN passing the checksum SHOULD be referred to as ‘checksum-valid’ and does NOT necessarily exist. It MUST NOT be considered otherwise valid.

In addition, for the purposes of efficiency pre-checkum validation MAY be executed. Such validation MAY based upon one or both of the length and structure of the IIBAN. An IIBAN passing such validation SHOULD be referred to as ‘structure-valid’ and does NOT necessarily exist. It MUST NOT be considered otherwise valid.

The only way to completely validate an IIBAN or IBAN is with the issuing institution.

6.3. IANA Processes

IANA MUST provide adequate authentication of registrant institution communications in order to prevent the subversion of established institutions’ registration information via IANA’s registrar
functions.

7. IANA Considerations

7.1. Institution Identifiers

7.1.1. Name Space Exhaustion

Should the entire ‘AA’ name space approach registration, IANA may look to subsume an additional [ISO3166] country prefix from those reserved by the ISO for user assignment.

7.1.2. Registration

Institution identifiers MUST be assigned by IANA on a first come first served basis [RFC5226]. Institution identifiers SHOULD NOT be provided to entities capable of issuing IBAN in conventional financial networks as this would represent duplicate allocation under the IBAN standard. Such entities MUST be defined as those offering banking services in countries that appear within the IBAN registry [IBAN-REG], with definitions of those terms being solely of IANA’s own judgement. Registrants MUST provide the domain name with which their service is primarily associated and the name of the registrant (either a person or an organizational entity). Registrants MAY provide a physical address, and MAY provide one additional identifier such as a business registration or license number.

Institution identifiers MUST be assigned randomly from the pool of available assignments and MUST NOT be granted on a specific request basis. Thus, the first issued institution code MUST NOT be ‘100’. Institutions unhappy with their random assignment for legitimate reasons (such as unfortunate linguistic connotations) MAY request one (1) replacement assignment. No further replacement is allowed. Registrants requesting replacement assignments automatically cause their initial allocation to expire (see Expiry, below).

7.1.3. Modification / Cancellation

Registrants MUST contact IANA to cancel or change the details associated with their registration. Authentication procedures will be stipulated at IANA’s discretion.
7.1.4. Expiry

In case of imminent name space exhaustion and no viable alternative avenues for expansion, IANA MAY consider the expiry of a registrant’s stated primary domain for a reasonable period (as determined by IANA) as adequate grounds for the deallocation of an institution identifier. Deallocated identifiers MUST be immediately returned to the pool of available allocations, and MUST be re-issued to new parties on a first come, first served [RFC5226] basis.

7.2. Publications

7.2.1. IIBAN Institution Identifier Registry

IANA SHALL publish revisions to the global registry of IIBAN institution identifiers as changes are made. The registry SHALL include date of registration and date of last modification of each record, in addition to registrant information and the assigned institution code.

7.3. ISO Liaison

On account of IIBAN’s exclusive use of IBAN’s reserved, user assigned name space, no ISO liaison should be required.

7.4. Security

IANA MUST provide adequate authentication of registrant institution communications in order to prevent the subversion of established institutions’ registration information via IANA’s registrar functions. As IANA is likely to have superior experience in this domain, specific procedures are left to IANA’s judgement.
8. References

8.1. Normative References


8.2. Informative References


9. Contributors

Thanh Luu <thanh@btcx.com>

10. Acknowledgments

* Payward Inc. funded the research and development of this document.

11. Authors’ Addresses

Walter Stanish
Payward Inc.
<walter@stani.sh>