ISO 7812/7816 Numbers and the Domain Name System (DNS)

<draft-eastlake-card-map-08.txt>

Donald E. Eastlake 3rd

Status of This Document

This draft is intended to be become an Informational RFC. Distribution of this document is unlimited. Comments should be sent to the author.

Abstract

There are a variety of servers, web pages, and the like, which holders of ISO 7812 financial transaction identification card (i.e., credit/debit card) numbers and ISO 7816 smart card or related numbers may need to locate on the Internet. For example, some systems assume a smart card holder can contact the issuer of a smart card application for maintenance and update functions and the payment protocols may assume that a card holder can locate the appropriate certification authority to obtain a card holder certificate. This document specifies a method using the DNS as an important element in locating card related facilities on the Internet by mapping ISO 7812 and ISO 7816 number systems into domain names.

Disclaimer

The methods proposed herein have not been endorsed by the issuers and registries of ISO 7812 and 7816 numbers.

Acknowledgment

Suggestions from the following persons, listed in alphabetic order, have been incorporated in this document and are gratefully acknowledged:

Doug Beattie, Electronic Commerce Consultants

Dave Burdett, Commerce One

Brian Carpenter, IBM

Robert Elz, University of Melbourne

Tony Lewis, VISA International

Table of Contents

1. Introduction

Financial transaction cards such as credit and debit cards are identified by numbers issued in conjunction with ISO standard 7812 [ISO 7812-1] and applications that run on ISO smart cards are identified by numbers issued in conjunction with ISO standard 7816 [ISO 7816-5]. In general, the leading digits of such numbers indicate the category and/or issuing institution and the remainder of the number provides further identification.

There has been no way, given such a number, to automatically find an Internet site related to the card issuer, the card brand, or other card facilities. Some operations in connections with smart card resident applications, such as resetting certain error conditions on a stored value card, may require contacting the issuer. Other protocols may require that other facilities based on card number be reached over the Internet.

A means of automatically mapping such identification numbers into domain names means that as soon as a number is known (due to user smart card insertion, the reading of a magnetic stripe, or user selection from a list of previous entered credit cards, for example), the ability would be present to easily attempt to contact facilities on the Internet for that number. Thus web browsers/wallets could provide "go to issuer", "go to brand", "get a certificate", etc., buttons whenever an IS0 7812/7816 identification number is known.

1.1 ISO 7812 Details

Under ISO 7812, card numbers are decimal and the first 6 digits are formally known as the Issuer Identification Number or IIN. This six digit prefix is sometimes referred to as the BIN (Bank Identification Number), although it applies to more than banks, and the entire number is sometimes known as the PAN (Primary Account Number), even though these numbers are also used for secondary accounts, Merchant accounts, and other account and identification numbers. Card numbers are frequently issued in connection with "brands" such as VISA, MasterCard, American Express, JCB, Discover, Dinners Club, Air Travel Card, etc.

Formally, ISO 7812 identification card numbers are divided as follows:

```
         1          2-6             7->        last
      +-----+-----------------+-----------+-------------+
      | MII | issuer identifier |           |             |
      +-----+-----------------+ account # | check digit |
      | issuer identification # |           |             |
      +-----------------------+-----------+-------------+
      |         ISO 7812 identification number          |
      +-------------------------------------------------+
        MII = Major Industry Identifier as follows
           0 - for ISO/TC 68 and other industry assignments
           1 - airlines
           2 - airlines  and other industry assignments
           3 - travel and entertainment
         4/5 - banking/financial
           6 - merchandizing and banking
           7 - petroleum
           8 - telecommunications and other industry assignments
           9 - for national assignment
```

If the number starts with 9, the next three digits are the numeric country code as defined in [ISO 3166] and the remainder of the number is as defined by that national standards body for that country.

Account numbers are variable length up to a maximum of 12 digits so the maximum total length is 19 bytes.

The check digit is calculated modulo 10 by the Luhn formula over all the preceding digits as specified in [ISO 7812].

The global registration agency for [ISO 7812] Issuer Identification Numbers is the American Bankers Association [ABA] but application for an IIN must generally be made through a national standards body.

1.2 ISO 7816 Details

ISO smart cards have applications on them each identified by a hexadecimal Application Identifier (AID) BCD encoded into a maximum of 16 bytes. In the past, most such cards have had a single application but multiapplication cards are expected to be more common in the future.

The first hex digit of the AID indicates the type of AID prefix as listed below followed by details on each type. In general, the AID prefix is followed a variable length "Proprietary application identification extension" (PIX) under the control of the issuer identified by the prefix.

0-9	An ISO 7812 IIN.
A	International registration.
B-C	Reserved for ISO.
D	National registration.
E	Reserved for ISO.
F	Proprietary non-registered

1.2.1 ISO 7816 '0'-'9' Prefixes

AIDs with a prefix of '0' through '9' use ISO 7812 IINs for the prefix (see section 1.1 above).

```
+-------------------------+--------+--------------------------+
|         ISO 7812        |        | Proprietary application  |
| issuer identification # |  'FF'  | identifier extension (PIX) |
+-------------------------+--------+--------------------------+
|            Application identifier (AID), 2-16 bytes         |
+-------------------------------------------------------------+
```

[ISO 7816] is designed to be independent of IIN length and specifies that if the IIN length is odd, it should be padded up the next full byte by suffixing a hex 'F' nibble.

1.2.2 ISO 7816 'A' Prefixes

In AIDs with a prefix of 'A' (i.e., binary 1010), the prefix is followed by 36 bits of Registry provider number as 9 BCD digits. Values in these 9 nibbles that do not corresponding to a decimal digits are reserved for ISO.

```
+-------------------------------------------------------+
|  Registered Application    | Proprietary application  |
| provider identifier (RID)  | identifier extension (PIX) |
|         5 bytes            |       <= 11 bytes        |
+-------------------------------------------------------+
|        Application identifier (AID), 1-16 bytes       |
+-------------------------------------------------------+
```

The registration authority for RIDs is [TELE DENMARK].

1.2.3 ISO 7816 'D' Prefixes

The RID consists of the 4 bit D prefix (binary 1101), the country code in 12 bits as 3 BCD digits coded according to the numeric country codes in [ISO 3166], and 24 additional bits as specified by the national standards body with BCD coding recommended.

```
      +---------------------------------------------------------+
      |  Registered Application    | Proprietary application    |
      | provider identifier (RID)  | identifier extension (PIX) |
      |         5 bytes            |       <= 11 bytes          |
      +---------------------------------------------------------+
      |        Application identifier (AID), 1-16 bytes         |
      +---------------------------------------------------------+
```

1.2.4 ISO 7816 'B', 'C', and 'E' Prefixes

Prefixes 'B', 'C', and 'E' are reserved for future use by ISO and not further specified.

1.2.5 ISO 7816 'F' Prefixes

Prefix 'F' indicates a proprietary non-registered AID. Because of this, the same 'F' prefixed AID could be used by different application providers for different applications.

```
      +------------------------------------------------------+
      |                  Application Label                   |
      +------------------------------------------------------+
      | Proprietary application identifier (AID), 1-16 bytes |
      +------------------------------------------------------+
```

2. Inverse Number Mapping and Wildcards

When numbers are allocated in lexically hierarchical blocks so that a prefix or suffix of digits is a meaningful division, the DNS wildcard feature can be used to provide a convenient delegation and lookup mechanism. This works even when the numbers and prefixes/suffixes are variable length. In this regard, it is important to remember that more specific names override less specific ones for DNS wildcards.

Domain names start with the most significant label on the right and go to less significant labels as you go left while in ISO 7812 and 7816 numbers the leading or left most digits are the most significant while the trailing or right most digits are less significant. Thus, the digits must be reversed to match the card number and DNS naming systems and the digits must be interspersed with dots to provide hierarchical division into DNS domains.

Note that the transformed, reversed number need not be exposed to users but could be generated internally by software in an automatic fashion.

[Note: while card.reg.int was assigned by IANA for this purpose, follwing the 10 May 2000 statement by the IAB, this may be changed to card.arpa or some other *.arpa.]

For example, currently the American Express card brand is the only one using [ISO 7812] numbers starting with 37. However, this is not a guarantee for all time and it could be that at some point some BIN numbers starting with 37 would be assigned to a different brand. If you are looking up facility "z" for card number 37012345678 (not a valid American Express number), you could do a retrieval with a name like 3.2.1.0.7.3.z.card.reg.int based on the first six digits of the number. A wild card RR with the name *.7.3.z.card.reg.int would match this and would appear in the response with its name expanded to the specific name asked for, but only if there were no more specific name. If there were a 3.2.1.0.7.3.z.card.reg.int specific name, for instance, it would always be chosen in preference to the *.7.3.card.reg.int wildcard in this case because it is a more exact match. Thus more specific values can punch out holes in ranges established by shorter, less specific prefixes. On the other hand, if a retrieval were done for 7.7.7.7.7.3.z.card.reg.int, it would get the more general *.7.3.z.card.reg.int wild card since it does not match the more exact wildcard. (The situation is generally a little more complex than indicted here because additional intermediate length wildcards may be needed. See the Appendix for a more complete example zone.)

3. Card Domain Names Specified

Subdomains are currently defined within the card.reg.int domain as follows in alphabetic order:

[Note: while card.reg.int was assigned by IANA for this purpose, follwing the 10 May 2000 statement by the IAB, this may be changed to card.arpa or some other *.arpa.]

```
acquirer.card.reg.int - ISO 7812 card acquirers
aid.card.reg.int      - ISO 7816 application identifiers
brand.card.reg.int.   - ISO 7812 card brands.
issuer.card.reg.int.  - ISO 7812 card issuers.
```

To find a facility, you need to (1) get the number, (2) reverse the order of these digits, and (3) put a dot between each digit and add the appropriate facility suffix. [ISO 7812] financial transaction card identification numbers generally must be truncated to six digits if revealing the full number in the DNS queries would be a security problem. Generally revealing the entire number in a DNS query is not a problem for [ISO 7816] AIDs.

None of the facility pointers obtained via these means need be exclusive and these card related Internet facilities may have other names and URLs that will also work. These facilities are intended to supplement, not necessarily replace, direct communication of domain names and URLs from financial institutions to their customers.

3.1 ISO 7812 Card Brand, Issuer, and Acquirer Pointers

The card brand and issuer home pages would be located by creating the numeric portion as above and appending ".brand.card.reg.int" or ".issuer.card.reg.int" respectively. A CNAME RR will be stored at that name pointing to the actual domain name for the home page. A CNAME is chosen, rather than having specific "A" RRs pointing to host(s), "MX" RRs pointing to mail servers, etc., to minimize the update load on the card.reg.int sub-domains. Changes in the serving host, mail servers, etc., need only be made under the facility's domain name, which the CNAME points to, rather than also under card.reg.int.

For example, the brand for the card 551204..., a MasterCard card, would be found by browsing at 4.0.2.1.5.5.brand.card.reg.int. and the issuer for the card 471922..., a VISA card, would be found by browsing at 2.2.9.1.7.4.issuer.reg.card.int. These domain names can be automatically generated from a card number and need not be exposed to users.

The Appendix shows possible initial content of the brand.card.reg.int domain. There are relatively few brands and they are allocated to moderately compact blocks of numbers with relatively few exceptions not belonging to the block brand. So there will probably be under 2,000 entries in the brand.card.reg.int subdomain.

Since there are only a few tens of thousands of banks and other issuers of significance in the world for financial transaction cards, there should be well under 200,000 entries in the issuer.card.reg.int subdomain.

Although at this time very large blocks of numbers are generally allocated to brands (for example almost all card numbers starting with 5 and 4 are MasterCard and Visa cards, respectively), some numbers within these large blocks may be carved out by more specific entries for other brands.

3.2 ISO 7812 Acquirer Facilities

Generally, merchants are assigned merchant IDs from the space of PANs by their acquirer. Acquirer facilities can be located from such numbers using the .acquirer.card.reg.int suffix.

3.3 ICON Location

For many of the facilities locatable via card.reg.int, some user interface software will want to be able to display an image or icon. Standard suffixes to the computed domain name of the facility are recommended, as listed below, to make the default location of such icons easier.

Suffix to Domain Name	Image Size in Pixels
/icons/exsmall.gif	32 x 32 or 32 x 20
/icons/small.gif	53 x 33
/icons/medium.gif	103 x 65
/icons/large.gif	180 x 114
/icons/exlarge.gif	263 x 166

The larger dimension above is horizontal and the smaller is vertical. The extra small version is permitted to be a 32x32 square which is a common desk top operating system icon size. It is recommended that displaying the extra small size be avoided due to lower recognizability is such small images. The color palette of the icons should be limited to colors typically available in an 8 bit or 256 color environment.

The above file name, size, and color recommendations are similar to those in Book 2 of the SET standards [SET].

3.4 Similar Proprietary Systems

Some proprietary systems use numbers schemes similar to [ISO 7812] or [ISO 7816]. For instance, an "Example" stored cash card system might use card IDs that have the same structure and prefixes as [ISO 7812] card numbers. Such schemes are welcome to use the techniques described in this document for inverse look up via DNS but should place the inverse tree under their proprietary domain name. For instance, the hypothetical stored cash card system could use ....card-number.example.com.

3.5 ISO 7816 Application IDs

Facilities based on [ISO 7816] application identifiers can be found using the

suffix. While a subset of such IDs are structured like ISO 7812 PANs, nevertheless, they are likely to need different facilities so no reference is made to the parts of the card.reg.int DNS tree allocated for non-smart card use.

4. Financial Institutions Not On Line

Some numbers may be allocated to institutions that do not have a network presence. In some of those cases, a wildcard could provide an appropriate pointer, say to a brand supplied bank lookup page that provides telephone number and address or the like to contact the bank. However, in cases where the next higher level wildcard would provide inappropriate pointers for such institutions, it will be necessary to add entries for such numbers which are CNAMEed to "not-on-line.card.reg.int" which will not exist. Thus an appropriate error message will be generated.

5. ISO 7812 BIN Ambiguity

For the facilities under card.reg.int using ISO 7812 numbers, the BIN is defined as the first six digits of the account number. In many cases an issuer or certification authority is defined by fewer digits, for example the first four digits. This is no problem as a wild card can be used to match all extensions of this shorter prefix. However, cases where six digits are insufficient need special handling as describe below. Such situations can arise due to subdivision / subdelegation of a BIN for administrative reasons, due to sale of part of a card population, as parts of bank mergers and splits, etc. Additional digits can not be used in the DNS query because they would reveal too much of the card number and thus be a security risk.

If multiple institutions have decided to share a BIN, there are several ways the situation can be handled. For the issuer web page either (1) the institutions sharing the BIN can run a common web page with links to their individual pages on it or (2) if they are all the same brand, the brand can run such a multi-issuer referral page at the BIN or, in many cases, at a higher level wildcard or (3) in the event that they are different brands, the card.reg.int maintainer can run a page providing access to the different sub-BIN issuers. A multiple issuer home page could just have names, icons, and links to the separate institutions or more complex indexing or search facilities if it covered many banks. While this problem in not expected to arise for the brand.card.reg.int subdomain, similar solutions apply if it does.

6. Security Considerations

This document concerns a means to map ISO 7812 financial card and ISO 7816 smart card application identification numbers into the Domain Name System (DNS) so that card related facilities on the Internet can be automatically located. The security of the resulting pointers is dependent on the integrity of the maintainer of the domain used for this purpose and the security of the DNS, including the use of security extensions [RFC 2535]. However, note that when used in connection with many smart card application, certificate issuance, and payment schemes, the security mechanisms of the protocols used after communications is established provide strong protection against spoofing or compromise of sensitive information even if the DNS were subverted.

For currently existing types of ISO 7812 financial numbers, care should be taken in making DNS queries that an entire sensitive identification number is NOT used. Since DNS queries are not encrypted, this would expose the card number within the Internet. No more than the initial six digits may be used. (These consideration do not generally apply to numbers based on ISO 7816 application identifiers.)

References

[ABA] - <http://www.aba.com>
American Bankers Association
1120 Connecticut Avenue, N.W.
Washington, DC 20036 USA

+1-800-BANKERS

[ISO 3166] - Codes for the representation of names of countries.

[ISO 7812-1] - Identification card - Identification of Issuers.

[ISO 7816-5] - Identification card - Integrated circuit(s) cards with contacts - Numbering system and registration procedures of application identifiers

Note: The International Standards Organization web site is at <http://www.iso.ch>. Final ISO standards, such as 3166, 7812, and 7816, are not generally available on the Internet and usually must be purchased through national standards bodies.

[RFC 1034] - Domain Names - Concepts and Facilities, P. Mockapetris, November 1987

[RFC 1035] - Domain Names - Implementation and Specifications, P. Mockapetris, November 1987.

[RFC 2535] - Domain Name System Security Extensions, D. Eastlake, March 1999.

[SET] - Secure Electronic Transaction (SET) Specification, Version 1.0, May 31, 1997, available from <http://www.setco.org>.
Book 1: Business Description
Book 2: Programmer's Guide
Book 3: Formal Protocol Definition

[SET-EIG] - External Interface Guide to SET Secure Electronic Transaction, September 24, 1997, available from <http://www.setco.org>.

[TELE DENMARK] - <http://www.teledanmark.dk>,
Tele Denmark
Attn: ISO/IEC 7816-5 Registration Authority
Teglholmsgade 1
1790 Copenhagen V
Denmark

Author's Address

Donald E. Eastlake 3rd
Motorola
155 Beaver Street
Milford, MA 01757 USA

Telephone: +1 508-634-2066 (h)
+1 508-261-5434 (w)
FAX: +1 508-261-4447 (w)
EMail: Donald.Eastlake@motorola.com

Expiration and File Name

This draft expires August 2001.

Its file name is draft-eastlake-card-map-08.txt.

Appendix: Initial ISO 7812 Brand Pointers

This table shows possible initial brand name pointers that might be installed in the brand.card.reg.int domain.

[In light of the 10 May 2000 IAB statement on infrastructure domains, card.reg.int may be changed to card.arpa or other *.arpa.]

Initial Name	CNAME
*.brand.card.reg.int	unknown-brand.card.reg.int
*.1.brand.card.reg.int	www.air-travel-card.com
*.3.brand.card.reg.int	unknown-brand.card.reg.int
*.0.3.brand.card.reg.int	www.dinersclub.com
*.6.0.3.brand.card.reg.int	www.dinersclub.com
*.9.6.0.3.brand.card.reg.int	www.jcb.co.jp
*.8.0.3.brand.card.reg.int	www.dinersclub.com
*.8.8.0.3.brand.card.reg.int	www.jcb.co.jp
*.1.3.brand.card.reg.int	www.jcb.co.jp
*.3.3.brand.card.reg.int	www.americanexpress.com
*.3.3.3.brand.card.reg.int	www.americanexpress.com
*.7.3.3.3.brand.card.reg.int	www.jcb.co.jp
*.5.3.brand.card.reg.int	unknown-brand.card.reg.int
*.2.5.3.brand.card.reg.int	unknown-brand.card.reg.int
*.8.2.5.3.brand.card.reg.int	www.jcb.co.jp
*.6.3.brand.card.reg.int	www.dinersclub.com
*.7.3.brand.card.reg.int	www.americanexpress.com
*.8.3.brand.card.reg.int	www.dinersclub.com
*.4.brand.card.reg.int	www.visa.com
*.5.brand.card.reg.int	www.mastercard.com
*.6.brand.card.reg.int	unknown-brand.card.reg.int
*.0.6.brand.card.reg.int	unknown-brand.card.reg.int
*.1.0.6.brand.card.reg.int	unknown-brand.card.reg.int
*.1.1.0.6.brand.card.reg.int	www.novus.com

(MasterCard actually only has numbers starting with 51 through 56 but until some other brand with cards issued with ISO 7812 numbers starting with a 5 are entered into the DNS zone, there is no reason to go to any more detail in the wildcard.)