Mapping Financial Transaction Card Numbers into the Domain Name System

---

Donald E. Eastlake 3rd

Status of This Document

This draft, file name draft-eastlake-card-map-00.txt, is intended to be become an Informational RFC concerning utilization of the Domain Name System (DNS) to support automated location of financial transaction card related facilities in the Internet. Distribution of this document is unlimited. Comments should be sent to the SET protocol development mailing list <set-dev@terisa.com> or to the author.

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ‘‘working draft’’ or ‘‘work in progress.’’

To learn the current status of any Internet-Draft, please check the lid-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net (East USA), ftp.isi.edu (West USA), nic.nordu.net (North Europe), ftp.nis.garr.it (South Europe), munnari.oz.au (Pacific Rim), or ftp.is.co.za (Africa).
Abstract

The SET protocol being developed by the VISA and MasterCard associations and others assumes that a financial transaction cardholder can locate the appropriate certification authority to obtain a cardholder certificate. This document proposes a method using the DNS and, in some cases the referral features of the SET protocol, to locate such certification authorities and other financial transaction card related facilities on the Internet by mapping ISO 7812 derived card numbers into domain names within in the card.int domain.

Disclaimers

The methods proposed herein are not, at the time of the issuance of this draft, specifically endorsed by the credit card brands or associations.

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

Tony Lewis, VISA International
Table of Contents

Status of This Document........................................1

Abstract.......................................................2
Disclaimers...................................................2
Acknowledgment.............................................2

Table of Contents...........................................3

1. Introduction..............................................4

2. Inverse Number Mapping and Wildcards....................5

3. Card Domain Names Specified..............................6
   3.1 Card Brand and Issuer Pointers.....................6
   3.2 Certification Authority (CA) Pointers...............7
   3.3 Financial Institutions Not On Line..................8
   3.4 BIN Ambiguity.........................................8

4. card.int Domain Maintenance Agency.......................10

5. Security Considerations................................11

References....................................................11

Author’s Address.............................................12

Expiration and File Name..................................12

Appendix: Initial Brand Pointers...........................13
1. Introduction

Financial transaction cards such as credit cards and debit cards are identified worldwide by numbers issued in conjunction with ISO standard 7812 [ISO 7812]. In general, the leading digits of such card numbers, formally called the Issuer Identification Number, indicate the issuing financial institution and the remainder of the number identifies the individual cardholder. The institution prefix is usually referred to as the BIN (Bank Identification Number) and the entire number is known as the PAN (Primary Account Number). Card numbers are generally issued in connection with "brands" such as VISA, MasterCard, American Express, JCB, Discover, Dinners Club, Air Travel Card, etc.

There has been no automatic way, given a card number, to find any Internet site related to the card issuer, the card brand, or other card facilities. In particular, the SET protocol [SET] defined by VISA, MasterCard, and others, defines a means for cardholders, when required, to obtain X.509 like certificates to attest to the cardholder’s authenticity but does not specify how to locate the appropriate certification authority.

In many cases, cardholders will be given URLs in mailings from the card issuer or on their card itself. However, there will be other cases, such as older cards that have not been updated to have a URL or for which the URL has changed due to bank mergers or splits or a previously registered card for which the certificate is expiring but the card is still valid, when access to the current URL is inconvenient. There may be cases where the URL has changed since a card was printed due to DNS changes. Furthermore, in certification authority interaction, the user will be required to supply their PAN in any case and the requirement that they manually enter a URL means additional effort and opportunity for error. (Note that PANs normally have a built in check digit to catch most typographical errors while URLs do not.)

A means of automatically mapping BIN numbers into domain names in most cases means that as soon as a BIN is known (due to user PAN entry or selection for a list of previous entered PANs, for example), the ability would be present to contact facilities on the Internet for that card. Thus web browsers/wallets could provide "get a SET certificate", "go to issuing bank", "go to card brand", etc., buttons whenever a BIN is known.
2. Inverse Number Mapping and Wildcards

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

Since domain names start with the most significant label on the right and go to less significant labels as you go left while in card numbers the leading or left most digits are the most significant while the trailing or right most digits are less significant, 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 card number need not be exposed to users but could only exist internally.

For example, currently the American Express card brand is the only one using numbers starting with 37. However, this is not a guarantee and it could be that at some future point some BIN numbers starting with 37 would be assigned to a different brand. If you are looking up card number 37012345678 (not a valid American Express number), you could do a retrieval with a name like 3.2.1.0.7.3.xy (to avoid exposing the credit card, no more than six digits may be included in the query). A wild card RR with the name *.7.3.xy 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.xy wild card, for instance, it would always be chosen in preference to the *.7.3.xy wildcard in this case because it is a more exact match. On the other hand, if a retrieval were done for 7.7.7.7.7.3.xy, it would get the more general *.7.3.xy wild card since it does not match the more exact wildcard.
3. Card Domain Names Specified

Subdomains are defined within the card.int domain for access to the card certification authority, the card issuer, and the card brand.

To find a facility, you need to (1) get the BIN, usually by truncating the PAN to its first six digits, (2) reverse the order of these digits, and (3) put a dot between each digit and add the appropriate facility suffix as shown below. The financial transaction card number is always truncated to avoid revealing the full PAN in the DNS queries.

Sections 3.1 and 3.2 give further details on the facilities available, section 3.3 discusses what to do about banks which are not on line, and section 3.4 discusses what to do if the BIN is too specific or not specific enough.

None of the facility pointers obtained via these means are meant to be exclusive and these financial transaction card related Internet facilities will normally have other names and URLs that will also work. These facilities are intended to supplement, not replace, the direct communication of domain names and URLs from banks to their cardholders, particularly in automated case.

3.1 Card Brand and Issuer Pointers

The card brand and issuer home pages can be located by truncating and reversing the number as above and appending ".brand.card.int" or ".issuer.card.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 brand.card.int subdomain. Changes in the serving host, mail servers, etc., need only be made under the brand’s domain name rather than also under card.int.

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

Appendix A shows an initial content of the brand.card.int subdomain. 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 1,000 entries in the brand.card.int subdomain.
Since there are only a few tens of thousands of banks of significance in the world for financial transaction cards, there should be well under 100,000 entries in the issuer.card.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), numbers within these large blocks can be carved out by more specific entries for other brands where necessary.

### 3.2 Certification Authority (CA) Pointers

A very high level description of the cardholder certificate issuance procedure in SET [SET] is for a cardholderCInitRequest initialization message to be sent to the CA, an initialization response received, then a registration form request to be sent and a registration form returned which the user fills in. The completed registration form is submitted in a certificate request message to which there is a response which can include the certificate or indicate it will be issued later. The registration form response message can also be a referral to another CA site rather than a registration form.

The above sequence can occur over a variety of transports [SET-EIG] including TCP and HTTP. TCP would be to the SET well known port 257, unless some other port was mutually agreed on, but cardholder to CA communication is normally expected to be HTTP. In HTTP, the sequence is usually preceded by a kick-off message from the CA which is of MIME type Application/Registration-Initiation which activates a SET wallet.

There are three pointers provided in connection with CAs, one for the CA general web page for browsing, one derived URL that can be hit to produce the SET certificate issuance kick-off message, and a derived URL that can be used to post the initial cardholderCInitRequest if a kick-off cycle is not needed.

The certification authority home page can be found as described in 3.1 above for brands and issuers, except that the suffix is ".SET-CA.card.int". A CNAME will also be used in this subdomain. At this time it is not clear in how many cases a certification authority will correspond to a single BIN, to a brand, to blocks of BINs, or even to part of a BIN (see section 3.4). Note that the wild card mechanism can easily accommodate arrangements such as a default certification authority for a brand with specific CAs for some BINs within that brand.

To determine the URLs to hit for the SET certificate issuance wake up message [SET-EIG], take the CA domain name as above, prefix it with...
"http://", and suffix it with "/Registration-Initiation". For some purposes, the wake up message may not be necessary. In that case, the cardholderCInitRequest SET message [SET] can be POSTed directly to a similar URL but with the suffix of /cardholderCInitRequest.

<table>
<thead>
<tr>
<th>Suffix to Domain Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Registration-Initiation</td>
<td>Certificate Request Wakeup</td>
</tr>
<tr>
<td>/cardholderCInitRequest</td>
<td>SET msg to start cert. req.</td>
</tr>
</tbody>
</table>

Note that no explicit DNS retrieval is necessary. In initiating a cardholder certificate application for card number 9876543210, you mechanically transform the PAN into a URL and go. In this case that would be, to start with a kick-off, <http://5.6.7.8.9.SET-CA.card.int/Registration-Initiation>.

3.3 Financial Institutions Not On Line

Some numbers are allocated to banks that do not have a network presence. To avoid inappropriate pointers for such banks, it will be necessary in some cases to add entries for such numbers which are CNAMEed to "bank-not-on-line.card.int" which will not exist. Thus an appropriate error message will normally be generated.

3.4 BIN Ambiguity

For the purposes of this document, the BIN is defined as the first six digits of the PAN. In many cases an issuer or certification authority is defined by fewer 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.

If multiple institutions have decided to share a BIN, there are several ways it can be handled. For the issuer web page either (1) the banks 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 some cases, at a higher level wildcard or (3) if they are different brands, the card.int maintenance agency (see section 4) 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 if it covered many banks.

The cases where a URL is derived to access certification authority
facilities are not logically different from the home page case but need a different implementation. In particular, instead of a human looking at a web page, we may have an application trying to get a cardholder certificate. However, when the registration process reaches the point of sending the CA a registration form request, that request is accompanied (securely) by the full PAN. The registration form response can have, instead of a registration form, a referral to a different URL. Thus, the "CA" could be simply a secure referral program that uses as much of the PAN as it wishes, possibly more than the first six digits, to determine where to forward the cardholder application. This referral CA could be, as in the home page case, run by multiple banks or a brand or the card.int maintenance agency (see section 4).
4. card.int Domain Maintenance Agency

For full operational deployment of the card.int domain, a maintenance agency for the DNS information will need to be identified.

A possibility is an existing company engaged in domain name registration activities or a newly created organization for this purpose. Also, the American Bankers Association (ABA) is the ISO 7812 registration agency and so is a natural possibility.

Funding for maintenance should not be a problem. Current going rates for large scale domain registration are $35 (US) or equivalent (NSI fee less 30% infrastructure fund deduction, rate change for registration in multiple third level domains under .card.int, it is hard to see how the annual cost for domain registration could be such that it would exclude any bank wishing to participate.
5. Security Considerations

This document concerns a means to map financial card numbers into the Domain Name System (DNS) so that card related facilities on the Internet, including the SET [SET] certification authority associated with the card, can be automatically located. The security of the resulting pointers is dependent on the integrity of the card.int maintenance agency and the security of the DNS, including the use of security extensions [RFC 2065]. However, note that when used in connection with SET certificate issuance, the SET security mechanisms provide strong protection against spoofing or compromise of sensitive information even if DNS were subverted.

Care should be taken in making DNS queries that the entire card number is NEVER used as this would expose the card number within the Internet. No more than the initial six digits, which constitute the BIN for the purposes of this document, can be used.

References


  Book 1: Business Description
  Book 2: Programmer’s Guide
  Book 3: Formal Protocol Definition

Author’s Address

Donald E. Eastlake 3rd  
CyberCash, Inc.  
318 Acton Street  
Carlisle, MA 01741 USA

Telephone:   +1 978 287 4877  
+1 703 620-4200 (main office, Reston, VA)  
FAX:           +1 978 371 7148  
EMail:         dee@cybercash.com

Expiration and File Name

This draft expires 29 March 1998.

Its file name is draft-eastlake-card-map-00.txt.
Appendix: Initial Brand Pointers

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

<table>
<thead>
<tr>
<th>Initial Name</th>
<th>CNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.1.brand.card.int</td>
<td><a href="http://www.air-travel-card.com">www.air-travel-card.com</a></td>
</tr>
<tr>
<td>*.0.3.brand.card.int</td>
<td><a href="http://www.dinersclub.com">www.dinersclub.com</a></td>
</tr>
<tr>
<td>*.8.8.0.3.brand.card.int</td>
<td><a href="http://www.jcb.co.jp">www.jcb.co.jp</a></td>
</tr>
<tr>
<td>*.9.6.0.3.brand.card.int</td>
<td><a href="http://www.jcb.co.jp">www.jcb.co.jp</a></td>
</tr>
<tr>
<td>*.1.3.brand.card.int</td>
<td><a href="http://www.jcb.co.jp">www.jcb.co.jp</a></td>
</tr>
<tr>
<td>*.3.3.brand.card.int</td>
<td><a href="http://www.americanexpress.com">www.americanexpress.com</a></td>
</tr>
<tr>
<td>*.7.3.3.3.brand.card.int</td>
<td><a href="http://www.jcb.co.jp">www.jcb.co.jp</a></td>
</tr>
<tr>
<td>*.8.2.5.3.brand.card.int</td>
<td><a href="http://www.jcb.co.jp">www.jcb.co.jp</a></td>
</tr>
<tr>
<td>*.6.3.brand.card.int</td>
<td><a href="http://www.dinersclub.com">www.dinersclub.com</a></td>
</tr>
<tr>
<td>*.7.3.brand.card.int</td>
<td><a href="http://www.americanexpress.com">www.americanexpress.com</a></td>
</tr>
<tr>
<td>*.8.3.brand.card.int</td>
<td><a href="http://www.dinersclub.com">www.dinersclub.com</a></td>
</tr>
<tr>
<td>*.4.brand.card.int</td>
<td><a href="http://www.visa.com">www.visa.com</a></td>
</tr>
<tr>
<td>*.5.brand.card.int</td>
<td><a href="http://www.mastercard.com">www.mastercard.com</a></td>
</tr>
<tr>
<td>*.1.1.0.6.brand.card.int</td>
<td><a href="http://www.novus.com">www.novus.com</a></td>
</tr>
</tbody>
</table>

(MasterCard actually only has numbers starting with 51, 52, 53, 54, 55, and 56 but until some other brand actually has cards issued with a number starting with a 5, there is no reason to go to any more detail in the wildcard. Discover/Novus could similarly be reduced to *.6.brand.card.int but in that case there would be no savings in number of entries in the zone.)