Universal Payment Preamble

---

Status of This Document

This draft, file name draft-eastlake-universal-payment-01.txt, is intended to be become a Proposed Standard RFC. Distribution of this document is unlimited. Comments should be sent to the author <dee@cybercash.com> or the ietf-payments@cc.bellcore.com mailing list.

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 Internet is becoming an increasingly commercial arena in which payments are rendered for goods and services. To support such commerce, numerous incompatible Internet payment protocols have been adopted by a variety of organizations. There appears to be little prospect of merger or abandonment of many of these protocols, none of which is currently under the change control of the IETF or any other standards body.

A universal payment preamble is proposed whereby parties can choose between this babble of alternatives.

Acknowledgements

The contributions of the following persons to this draft are gratefully acknowledged:

Randy Bush <randy@psg.com>
Steve Crocker <crocker@cybercash.com>
Bill Melton <melton@cybercash.com>
Paul-Andre Pays <pays@gctech.edelweb.fr>
Table of Contents

Status of This Document...........................................1
Abstract..........................................................2
Acknowledgements................................................2
Table of Contents................................................3
1. Introduction..................................................4
  1.1 Protocol Wars..............................................4
  1.2 Freedom to Shop..........................................5
  1.3 The Universal Payment Preamble Solution.................5
2. The Universal-Payment Preamble..............................6
  2.1 The Universal-Payment Message............................6
    2.1.1 Universal-Payment Formats............................6
    2.1.2 Definition of Acceptable Field Values.................8
    2.1.3 Transport of Universal-Payment Via HTTP..............9
    2.1.4 Transport of Universal-Payment Via email...........9
  2.2 The Turn-Around Message.................................10
  2.3 Message Integrity.......................................11
3. Anticipated Effects of Universal Payment Preamble......12
4. Potential Long Term Issues.................................13
5. Security Considerations....................................14
References......................................................14
Author’s Address...............................................14
Expiration and File Name....................................15
1. Introduction

Note: This draft does not necessarily reflect either a CyberCash corporate position or a description of any existing CyberCash product.

The Internet is becoming an increasingly commercial arena in which payments are rendered for goods and services. This commerce can take a variety of forms from shopping interactively with a World Wide Web browser to ordering by email from a CD-ROM catalog. Typically the shopping phase is followed by a payment phase and then sometimes by a fulfillment or delivery phase.

To provide general privacy and security to all three phases, there are a variety of IETF standardized protocols, such as MOSS or IPSEC, and other protocols, such as PGP, S-HTTP, SSL, or PCT. Some people use such general secure channel or secure message systems for payments. However, the payments phase is especially sensitive due to dealing with "real money", thus providing a strong incentive to crackers, and is also especially complex, frequently involving three parties such as a customer, merchant, and bank, with structured and interlocking messages that incorporate fields best encrypted for parties other than their initial recipient. For these reasons a number of specialized payment protocols have been adopted.

1.1 Protocol Wars

Note: "The best thing about standards is that there are so many to choose from."

As examples of payment protocols, MicroSoft (which controls the operating system of about 80% of the computers in the world) and VISA (the largest bankcard association) recently announced STT and Netscape (which controls the web browser of about 80% of the web users in the world) and MasterCard (the 2nd largest bankcard association) announced SEPP. Although both have some hopes of agreeing on a common protocol, these two systems are completely incompatible with each other and each is completely incompatible with every existing deployed system such as First Virtual or CyberCash. And there are numerous other systems and proposals, such as CMU’s NetBill, a proposed service by VeriFone, and many more.

All of the above mentioned payment protocols, even those which have been proposed as IETF standards, are currently under the exclusive control of their authors and none is even before an IETF Working Group.
1.2 Freedom to Shop

Some of the most prominent proposals seem designed to move the customer's decision as to payment system as early as possible. STT urges that STT proprietary credentials be used from the very start of any customer to merchant communications. Such a strategy is understandable as, from the point of view of a proponent of one the these systems, it is desirable to get the earliest possible lock-in.

But this is not what people do in real life and not what they want to do on the Internet. People want to shop and browse without commitment and then select among the alternative payment means after they have selected their purchase and are generally satisfied with the price and terms.

True, if they want privacy in shopping, they need to have a secure channel to the merchant. But the apparent bindings between secure channel technology and payment systems is false. There is no good reason someone could not speak the MasterCard SEPP protocol over a MicroSoft PCT channel or send CyberCash messages over SSL channels.

1.3 The Universal Payment Preamble Solution

A high level overview of the Universal Payment Preamble solution to this problem is as follows:

Shopping proceeds in a completely free-form way constrained only by the desires of the customer and merchant. After the order has been decided on, the definitive order and payment options are transmitted from the party knowing them to the other. The party receiving this message chooses the payment option (in general choosing transport protocol, payment system, payment type, etc.) and proceeds using the selected payment system, if any of those presented are acceptable.
2. The Universal-Payment Preamble

The Universal-Payment Preamble consists of two messages, the Universal-Payment Message and the Turn-Around message which are described below.

Normally only the Universal-Payment Message is required and the recipient of the Universal-Payment message can then initiate the payment system they selected from the options list in that message. However, should the selected payment system require that the party sending the Universal-Payment message also send the first message in the selected payment system, the receiver of the Universal-Payment message can use the Turn-Around message to prompt the sender to start the payment system message sequence.

2.1. The Universal-Payment Message

The Universal-Payment message has three purposes, (1) payment system independent mutual knowledge of order information at both the customer and merchant, (2) a smooth transition from whatever shopping dialog the customer engaged in to a specific payment system over a particular transport, and (3) a smooth transition back to any subsequent fulfillment dialog.

In almost all cases, the shopping dialog between the customer and the merchant will have resulted in the creation of an "order" and pricing information. This order and pricing information is normally only present at the merchant or the customer as of the end of the shopping dialog. For example, if the customer has been interacting via a browser with a merchant’s web service, the order (or shopping basket or whatever other term you like) and price has been accumulated at the merchant. If the customer has been interacting with a local CD-ROM catalog or the like, then the order and pricing will have been accumulated at the customer. The Universal-Payment message is then sent from the party with knowledge of the ordering information to the part without that knowledge. In addition, the message announces the available combinations of payment systems, payment messages transport protocols, payment types (credit, cash, etc.), and the like.

2.1.1 Universal-Payment Formats

On necessity, the exact form of the Universal-Payment message (UPM) must depend on the transport medium that it is sent over. However, in all cases, it contains the order and payment information. It may optionally contain expiration and/or continuation information.
order: This is the accumulated description of the good and services that have been ordered.

In several protocols, there is a need to convey the Goods and Service (GSO) order, out of band to the actual protocol. The order in the UPM is intended to provide a primary and unambiguous transport for this information.

In addition, the GSO must ultimately be cryptographically signed and compared in most of these protocols. To this end, it is essential that the GSO be conveyed exactly because the hash and signatures will not work if there is any change.

In email and World Wide Web transmissions, the content-transfer-encoding field defines the encoding of the body of the message and the content-type field defines the type. If the type of the GSO is text/plain with sufficiently short lines, then the encoding may be omitted. (It is recommended that any hashes calculated be on the text with all whitespace ignored, but this is the realm of individual payment protocols.) If the GSO is anything other than text/plain or there is any question of it being corrupted by a gateway, then the content-transfer-encoding should be be base64 to preserve the integrity of the message.

The GSO need not be machine parsable and in fact is simply a representation of the order for the records of the customer and the merchant. It would normally contain a description of the goods and/or services ordered and some information on delivery. Except perhaps if the customer were some automated process, the order should be easy for a person to understand. It might also include an order number, dates, prices, and the like but these would not generally be extractable from the order. For example, although text would be more common, the order might be a synthesized digitized voice reciting the information (this might be particularly useful for a blind customer) or an image of a completed illustrated order form.

WARNING: Since the order is what the customer is buying as a matter of record, it is essential that it be complete unto itself. External references are invalid in the sense that they can not be depended on later in showing what the order was. Thus an external MIME reference is prohibited as the order (or as part of the order if it is multipart), external references to images or otherwise are prohibited if the order or part of a multipart order is type text/HTML, etc.

payment: This is the pricing, payment systems, transport protocol, payment type, and similar information. In particular, it indicates what combinations of these are acceptable to the party sending the Universal-Payment message. It is intended for
automated processing and it need not be easily understood by a person. While the price will typically be the same for various payment methods, it might differ. Payment parameters are indicated by case insensitive digraphs as follows (in alphabetic order):

AM = amount (12.34)
CC = credit card type
CU = currency in ISO 4217 format (cad, jpy, usd, ...)
ID = payment system specific order identifier provided by merchant.
PS = payment system (CyberCash, FirstVirtual, SEPP, STT, ...)
PT = payment type (cash, credit, debit)
TP = transport protocol (a URL specifying protocol and address)

Parameters are separated by commas and alternatives are grouped with square brackets ("[]") and separated with vertical bar ("|").

continuation: This optional field contains information on where the user should be directed after the payment protocol. It may only occur if the Universal Payment Message is being sent by the merchant.

It consists of any one or more of the case insensitive keywords SUCCESS, FAILURE, and CANCELLATION, followed by an equal sign and a URL indicating where the user should go if the specific payment protocol being used ends the way specified by the key word. If more than one appears, they are separated by commas.

expires: This optional field specifies the date on which the offer represented by the Universal Payment Message expires. Under many legal systems, the absence of an expires field and explicit text in the GSO or elsewhere would mean that the offer expires in a reasonable length of time under the circumstances.

2.1.2. Definition of Acceptable Field Values

Some of the fields in the payment section have been explicitly defined. Most fields must support open ended addition of new designated names. Specifically the PS field must support (at a minimum) the current major payment protocol options: SEPP, STT, FirstVirtual, CyberCash, NetBill, DigiCash, NetCheque, ...

Similar issues affect PT though the choices are more limited there.

To support this need, we propose that IANA will maintain a registry of payment system names as is done for MIME types.
2.1.3 Transport of Universal-Payment Via HTTP

When transmitted via HTTP as a reply, the Universal-Payment message has MIME type application/universal-payment. The body of the reply is a MIME message. This nested MIME message has as its body the order information and as its Content-Type, the actual type of the order information such as text/plain. The payment information and other optional fields are header lines.

HTTP/1.0 200 OK
MIME-Version: 1.0
Content-Type: application/universal-payment
Content-Length: nnn

Content-Type: text/plain; charset="us-ascii"
Payment: AM=20.00, CU=cad, TP=<http://orders.merchant.tld>,
        [[PS=SEPP, PT=credit, CC=MC] |
         [PS=STT, PT=credit, CC=VI] |
         [PS=CyberCash, ID=merchant=13,
            PT=credit, [ CC=DI | CC=AX ]]]

Order of 20 December 1996 from merchant, 321 Main Street:

One Audio CD "Payment Systems I have known" $20.00
    Plus shipping and tax                      5.43
    total  25.43
Ship to:  John Doe
         123 Last Street
         Toronto, Ont.

2.1.4 Transport of Universal-Payment Via email

When transmitted via mail, the Universal-Payment Message is a MIME message of type application/universal-payment. The body of this message is in fact a MIME message. This nested MIME message has as its body the order information and as its Content-Type the actual type of the order such as text/plain.

The following example shows a case where a user has created an order, possibly by interacting with an application from a CD-ROM catalog, and wishes to place the order with a merchant. This customer has software on their computer (possibly some installed on the same CD-ROM) supporting the CyberCash, SEPP, and STT protocols. They also have Diners Club, MasterCard, VISA, and American Express credit cards and are willing to pay in cash.

The following could be generated automatically for the customer to convey this information to the merchant. The merchant would then
initiate the payment system they chose. (The specification below that the payment system would use email as its transport presumes that each payment has been defined over that transport.)

From: customer@mythical.tld
To: merchant@mall.tld
Subject: purchase
MIME-Version: 1.0
Content-Type: application/universal-payment
Content-Type: text/plain; charset="us-ascii"

Payment: AM=130.00, CU=usd, TP=<mailto:customer@mythical.tld>,
(comment: will pay $US 130.00 and want payment via email)
[[ PS=SEPP, PT=credit, CC=MC ] |
 [ PS=STT, PT=credit, CC=VI ] |
 [ PS= CyberCash, ID=merchant-13, |
 [ PT=credit, CC=AX ] | PT=cash ] ]

Order of 15 December 1996 from ACME CD_ROM Catalog of July 1996:

<table>
<thead>
<tr>
<th>Qty</th>
<th>Item</th>
<th>Unit Cost</th>
<th>Projected Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rocket Shoes</td>
<td>$90.00</td>
<td>$90.00</td>
</tr>
<tr>
<td>4</td>
<td>Rocket Refills</td>
<td>10.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

TOTAL COST $130.00

Ship to: Wiley Coyote
123 Last Street
Springfield, ZZ 00000

2.2 The Turn-Around Message

If the party where the order information has accumulated and which sent the Universal-Payment Message (UPM) to the other party is also the party which is to send the first message under the selected payment system, then the other party must send a Turn-Around Message to start the payment protocol. The only required data in a Turn-Around message is the one selected set of parameters of payment systems, type, transport, etc. If the original UPM was from customer to merchant, then the Turn-Around Message may also contain continuation data and may contain an "ID" parameter in a "payment:" field.
2.3 Message Integrity

It is strongly recommended that the Content-MD5 header by used on both the Universal-Payment Message and the Turn-Around Message to protect against corruption in transmission. However, this does not provide security.

Since one of the purposes of the UPM is to negotiate protocols, most of which have different security and signature schemes, no explicit signature is provided on the UPM. If security of the UPM is desired, the customer and merchant need to communicate inside some security enveloping, such as IPSEC, MOSS, SHTTP, PGP, or SSL from the start. If such security is not used, a UPM message could be modified in flight or spoofed; however, later steps within the payment protocol chosen will normally catch such a problem, reducing it to more of an interference or denial of service threat.
3. Anticipated Effects of Universal Payment Preamble

While the introduction of yet another protocol has the potential to further disrupt the progress in Internet payments, the Universal-Payment Message described here is intended to provide a minimal layering that enables a customer to use a multipayment wallet and to easily move from payment to payment.

Without a Universal Payment Preamble, shoppers and merchants will be forced into dealing with a large number of relatively confusing choices early in the purchasing process. The merchant must provide multiple payment buttons (depending on protocol) and then handle each separately.

This is not practical. Any form of impediment to the customer will discourage a number of buyers. The introduction of the Universal payment protocol allows merchants to shop for payment systems that are appropriate to their customer base and needs. Adding payment systems will be painless for the customer as only choices appropriate to the customer need be displayed on the screen.

The long term effects of this approach will be to more effectively allow different payment systems to compete in an open market.
4. Potential Long Term Issues

There is much discussion on the use of more general extension protocols for negotiation similar to the need filled by the Universal Payment Preamble. We support this idea in concept. However, to speed the introduction of payment systems, this very simple approach is adequate and can be implemented almost immediately.

Many of the Wallet programs are implemented as add-on applications separate from the browsers, thus any extension protocol must support external viewers acting as Wallets.

As more general protocol extension mechanisms become widely available in browsers and other tools, use of the Universal Payment Preamble may be revisited.
5. Security Considerations

The Universal-Payment protocol provides no security features.

It is intended to segue into a payment protocol selected by the customer and merchant and it is assumed that this payment protocol will provide adequate security. If security of (1) the Universal Payment Preamble messages, (2) any dialog preceding those messages, or (3) any fulfillment dialog after the payment protocol is desired, then an appropriate channel or message security protocol such as IPSEC, SSL, MOSS, SHTTP, PGP, etc. should be chosen.

References

[CyberCash]
[Green Commerce]
[MIME]
[PGP]
[SEPP]
[STT]

Author’s Address

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

Telephone:   +1 508 287 4877
             +1 703-620-4200 (main office, Reston, Virginia, USA)
email:       dee@cybercash.com

Brian Boesch
CyberCash, Inc.
2100 Reston Parkway, Suite 430
Reston, VA 22091 USA

Telephone:   +1 703-620-4200
email:       boesch@cybercash.com
Expiration and File Name

This draft expires 5 May 1996.

Its file name is draft-eastlake-universal-payment-01.txt.