INTERNET-DRAFT
Expires: 19 September 1996

Donald E. Eastlake 3rd
CyberCash
20 March 1996

Universal Payment Preamble

Status of This Document

This draft, file name draft-eastlake-universal-payment-02.txt, is intended to be become a Proposed Standard RFC. Distribution of this document is unlimited. Comments should be sent to the author or to the <ietf-pay@imc.com> and <jepi-payments@commerce.net> mailing lists.

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 1id-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.

A unified payment syntax is presented for parties to negotiate payment alternatives at any point in shopping, until a final hand-off to a particular chosen payment system.

Acknowledgements

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

Ali Bahreman <ali@eit.com>
Brian Boesch <boesch@cybercash.com>
Randy Bush <randy@psg.com>
Steve Crocker <crocker@cybercash.com>
Rohit Khare <khare@w3.org>
Pieter van der Linden <vdl@GCTech.fr>
Bill Melton <melton@cybercash.com>
Jim Miller <jmiller@w3.org>
Paul-Andre Pays <pays@gctech.edelweb.fr>

Table of Contents

1. Introduction

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 interactiny with a vendor via a World Wide Web browser to ordering by email from a CD-ROM catalog. Typically the shopping or selection phase is followed by a payment phase and then usually 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 S-HTPP, PGP, and SSL. Some people use such general secure channel or secure message systems for payments. However, the payments phase is especially sensitive because it deals with "real money", thus providing a strong incentive to crackers, and is also especially complex. Frequently payment involves three or more parties such as a customer, merchant, and bank or payment system, 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.

As examples of payment protocols, there is the SET standard being developed by MasterCard and VISA, the CyberCash system [RFC 1898], GCtech's GlodeID, CMU's NetBill, and many more.

The Universal Payment Preamble provides three capabilities: (1) negotiation of payment service, (2) exchanage of payment related identification information, and (3) initiation of the specific payment system. The payment service and initiation information are sufficient to smoothly bridge from shopping to payment and, if appropriate, from payment back to other customer - vendor interaction.

1.1 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 free-form way constrained only by the desires of the customer and vendor. Some information closely related to shopping but not closely tied to payment is made available via changes in HTML so that certain specially named fields can be semi-automatically filled in with such information as shipping address. This includes such items as shipping address, customer name, telephone number, and email address. [The field names and HTML changes will be documented elsewhere.] If desired, UPP information

may be exchanged before or during the shopping process. This might

be done so the customer is assured they can pay by a means they want to use or so that a merchant can condition their offer based on information about the customer. After the order has been decided on, the definitive order and remaining payment options are transmitted from the party knowing them to the other in a initiation message. The party receiving this message chooses the payment option (in general choosing transport protocol, payment system, payment type, etc. to the extent these have not been decided by earlier negotiation) and proceeds using the selected payment system if any of those presented are acceptable.

2. The Universal Payment Preamble

The Universal Payment Preamble is so called because it exchanges information that needs to be resolved before a particular payment system is entered and provides an initiation message to enter the payment protocol. It is expected that it will frequently be used in conjunction with the profile protocol [draft-eastlake-pep-profile-00.txt] which can exchange ancillary information that may be important to some payment systems.

Information is exchanged using the Protocol Extension Protocol [draft-khare-http-pep-*.txt] headers. Familiarity with PEP is assumed in this draft.

2.1. The Universal Payment PEP Headers

Each payment system is considered to be a PEP protocol extension, identified by a URL, and in addition there exists the http://pep.w3.org/UPP protocol. Each payment system as well as the umbrella UPP protocol should register itself as handling its own protocol and also handling the UPP protocol. (Some payment systems may also wish to register for the Profile protocol. See draft-eastlake-pep-profile-00.txt.)

UPP headers can be exchanged before or during shopping to narrow the field of payment methods and gain some assurance that there is some acceptable method available. This will occur via PEP headers using the payment system and UPP protocols.

Each individual payment service will have a proprietary protocol compatible with the "generic" UPP Protocol. Compatibility is largely defined by the parameters defined in section 2.2 below that lists the names of common parameters and the encoding to be used for their values. In addition, it implies an agreement about a "style" of negotiation: the payee agrees not to take irrevocable action based solely on the use of the UPP and specific payment protocol negotiation. Rather, it takes place in the proprietary protocol that starts at the end of the negotiation phase. Payment security is attained to the extent it is provided by this proprietary protocol.

When a merchant says "I request UPP, optionally", it is asking the customer to generate a list of the clients' offered payment systems (or vice versa if the customer makes this request). The server demands payment by requesting 'UPP, strength=required.' This forces the client to respond with one or more 'armed' payment initiators (i.e. with all parameters for chosen payment system(s) filled in). If the negotiation process has not narrowed down to a single payment

system, the browser/UPP module may pop up a notification toolbar or

automatically choose or leave it to the server to either choose or force a choice by using an HTML form.

Requesting the UPP protocol is the same as asking the other party which payment services it has that it is willing to reveal. Requiring the UPP protocol is requiring the other party to tender a specific payment. Asserting a UPP protocol means that a protocol instance message is payment.

2.2 Special UPP Protocol Parameters

The following PEP parameters, if they appear in a params bag for a payment system, have the form and meaning indicated:

account: This parameter is used to provide information about the account number to be used at the customer or merchant. Usually this number is meaningful only for the particular payment system but account type information, such as card brand, may be given to indicate choices. For example "{params ... {account-type {AX} {MC} {VI}} ...}" to indicate that American Express, MasterCard and VISA are acceptable (vendor) or providable (customer). [brand-ids may need to be BINs or something more complex than this...]

amount: This is the cost of the order thus far. It consists of a list of bags with the ISO 4217 currency code as the first item and optionally an amount as the second. For example "{params ... {amount {usd} {gbp}} ...}" to indicate that US dollars and pounds Sterling are acceptable (vendor) or providable (customer) or "{params {amount {frf 1234}}}" to indicate a precise amount in French francs. A cost with amount(s) is usually transferred with or before the initiation message if payment of an amount is required.

transport: This is the URL to which the initial payment service specific message should be sent. Normally this field occurs only in the headers on the initiation message. For example "{http://paycompany.com/paysys {params ... {transport http://merchant.com:8000/buy}} ...}" or {http://cashco.com/cash {params {transport mailto://mailorder@merchant.com}}}".

success: This is the URL to continue at after successful execution of the payment protocol. Normally this field occurs only in the headers on the initiation message.

failure: This is the URL to continue at after failure of the payment protocol. Normally this field occurs only in the headers on the initiation message.

cancel: This is the URL to continue at if the payment protocol is cancelled. Normally this field occurs only in the headers on the initiation message.

2.3 The Initiation Message

There is a sharp transistion from the shopping phase, which may include payment system negotiation as above. This is usually signalled by the MIME type of a message, typically "application/paysys" where "paysys" is the name of the payment system being invoked. With UPP, in principle this payment system specific MIME type is not required as this message will also have a UPP header demanding use of the UPP protocol. But it is better pracrice to use the MIME type to ensure transition to the payment system without relying on the other parties UPP capabilities. The exact form nad body content of the initiation message depend on the payment system and the transport medium that it is sent over.

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 frequently 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 initiation message is sent from the party with knowledge of the ordering information to the part without that knowledge. In addition, the message can announce the available combinations of payment services, payment types (credit, cash, etc.), and the like if this has not been previously determined by UPP header exchange.

The header of the initiation message will contain an instance of the selected payment protocol requiring the other party to follow that payment protocol or indicate an error. The body of the initiation message will normally include the "order". This is the accumulated description of the good and services that have been ordered.

In addition, the goods and services order (GSO) must ultimately be cryptographically signed and compared in most payment 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. However, some payment systems have their own out of band solution to this problem.

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 body/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 body/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.

However transmitted, 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 vendor. 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.

2.4 UPP Header and Message Integrity

Since one of the purposes of the UPP is to negotiate between payment protocols, most of which have different security and signature schemes, no explicit security is provided in the UPP. If security of the UPP 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 UPP relevant field or 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. Examples

Three examples are given below. The first is a minimum UPP example where neither party reveals much, the second is an example of a richer basic UPP example including some use of the Profile protocol, and the third is a relatively complex example illustrating the effects of policy at the customer and vendor ends.

3.1 Minimal UPP Example

This is a web example with a minimum of negotiation and in which the customer does not reveal anything about their identity.

```
====================================
GET /catalog
Protocol-request: {http://pep.w3.org/UPP}
```

Above the customer asks the merchant to give back catalog data and to indicate whatever payment systems it will tell a putative stranger about.

```
====================================
206 Uses PEP
Protocol-request: {http://cybercash.com/Pay {for /} },
   {http://gctec.com/GlobeID  {params {affiliate Kleline Cyttybank
   Mitsushami } {for /}}
```

The merchant's server indicates that it accepts 1. CyberCash for all URLs 2. GlobeID protocol for all URLs, and, using GlobeID private parameters, it is affiliated with the services operated in France by Kleline S.A., in Japan by Mistushami and in the Netherlands by Cyttybank. The body of this message would be the HTML catalog and the customer would proceed to shop and the customer knows they can pay by either Globe ID or CyberCash.

3.2 More Generous UPP Example

The GlobeID system has many parameters that it can securely certify once one is in the proprietary payment system. In this example, many of these are passed during PEP negotiation as "hints".

The price or amount is not included in this negotiation because the knowledge or selection of other parameters is frequently required to set this value (eg. custom duties, VAT, special discount when using a given instrument, or special discount because the customer is buying

in the same shop for the third time in the same month and because

GCTech system tends to present the amount to be paid (not the price) in the last step when everything is known in a certified way because the offer is non-repudiable and notarized within the GlobeID system. (This is only an example and it is possible to present a price to the customer with PEP when payment is via GloveID. This is basicly up to the merchant.)

```
====================================
GET /catalog
Protocol-request: {http://pep.w3.org/UPP}

the merchant response can be

====================================
206 Uses PEP
Protocol-request: {http://cybercash.com/Pay {for /} },
   {http://gctec.com/GlobeID  {params {affiliate Kleline Cyttybank
   Mitsushami } {amount} {b2b}} {http://pep.w3.org/Profile {params
   {residence-country} {delivery-country} {str opt}}
Protocol: {http://pep.w3.org/Profile {params {language FR NL} {amount
   {USD} {FRF} {NLG}} {residence-country {FR}} {delivery-country
   "ANY"} }}
```

The merchant asks for a variety of identification information from the customer, including the GlobeID proprietary b2b (business-to-business) parameter. The merchant optionally asserts that it is French, can delivery anywhere, and can accept payment in US dollars, French francs, and Netherlands guilders.

Shopping proceeds and the customer eventually indicates how they will pay via a message with the following headers:

```
====================================
POST /buy
Protocol: {http://gctec.com/GlobeID  {params {affiliate Kleline}
   {account (Cid) 1234567} {amount {FRF} {NLG}  {b2b TRUE}}
   {http://pep.w3.org/Profile {params {residence-country FR}
   {delivery-country US}}}
```

The customer gives their GloveID CiD (account), affiliate, indicates that this is a business to business transaction by a French resident entity for delivery in the US with payment to be in French francs or Netherlands guilders.

3.3 Complex UPP Example

This is a moderately complex example using both the UPP and Profile

protocols. Assume the Merchant has CyberCash, FooCharge, and SET for

AmEx installed but is only willing to process AmEx charges over $20.

Assume the Customer has SET for MasterCard and VISA which they only use for charges over $10 but is their preferred method when available, GlobeID which they use for hard goods, CyberCash persona #3 which they only use for charges over $30 and FooCharge id #7 which they only use for charges under $45.

Note that while these policies affect each parties requests and responses, the policies as such never appear on the wire.

```
==================================
Get /catalog
Protocol-request: {http://aba.com/SET {params {account {MC} {VI} }}},
   {http://pep.w3.org/Profile {params {residence-country} {age}}{str
   req}}
Protocol: {http://pep.w3.org/Profile {params {age 12}}}
```

The default strength is optional and the default scope is origin. This is the initial request to the merchant to see their catalog. Because SET is preferred by the customer, they offer it and they also demand that the merchant state their country and age. The customer also states that their age is 12. To avoid sending out the MC/VI option in essentially every request, the customer might not do that until they got a Protocol-request from the merchant optionally specifying the UPP protocol.)

```
==================================
206 Uses PEP
Protocol-request: {http://cybercash.com/Pay {for /}},
   {http://foocharge.com/Pay {for /}}, {http://aba.com/SET {params
   {acct {AX} }}}, {http://aba.com/SET {params {acct {MC} {VI}} {str
   ref}}}
Protocol: {http://pep.w3.org/Profile {params {country bd} {age 69}}}
```

= HTML for catalog

The merchant indicates what payment systems it can accept and refuses the one offered by the customer. In addition, it answers the customer Profile demand.

```
==================================
```

User asks to see summary of order...

```
==================================
206 Uses PEP
Protocol-request: {http://cybercash.com/Pay {params {amount {usd 33}
```

```
      {bdr 4162}}}, {http://foocharge.com/Pay {params {amount {usd 35}
```

{bdr 4262} }}}, {http://aba.com/SET {params {account {AX}} {amount {usd 34} {bdr 4200} }}}, {http://pep.w3.org/UPP {str req} {for /Pay}}

= HTML - shopping cart contents
= amend-order-button cancel-button pay-button

When the user gets a page with a button/anchor on it the activation of which indicates they are willing to pay, that page has all the merchant available payment options that have not yet been refused by the customer and demands the use of the UPP protocol in the response if the response is to the URL indicating that the payment button has been hit (/Pay in this case).

==========
GET /Pay
Protocol-request: {http://cybercash.com/Pay {params {amount {usd 35} }},{http://foocharge.com/Pay {params {amount {bdr 4262} }}

This is what happens with no user interaction at the customer and circumstances such that more than one payment system would work. The amount options may be narrowed to the most advantageous but otherwise all the options are given back. More likely, the options would be presented to the user who would, in this case choose between CyberCash and foocharge or possibly cancelling.

==========
206 Uses PEP
Protocol: {http://foocharge.com/Pay {params {amount {bdr 4262} } {proprietary foo} {transport URL} {success URL} {Failure URL}}}
Content-type: application/foocharge

= body of message = = includes GSO =

4. 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 Preamble 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 Preamble 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.

5. Security Considerations

The Universal Payment Preamble 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 headers/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, MOSS, SHTTP, PGP, SSL, etc. should be used.

References

draft-khare-pep-*.txt

[RFC 1898] - CyberCash

[RFC 1521] - N. Borenstein, N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", 09/23/1993.

[RFC 1522] - K. Moore, "MIME (Multipurpose Internet Mail Extensions) Part Two: Message Header Extensions for Non-ASCII Text", 09/23/1993.

[PGP]

[SET]

Author's Address

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

Telephone: +1 508-287-4877
+1 508-371-7148 (fax)
+1 703 620-4200 (main office, Reston, Virginia, USA)
email: dee@cybercash.com

Expiration and File Name

This draft expires 14 September 1996.

Its file name is draft-eastlake-universal-payment-02.txt.

Appendix A: Card Brands

[The world is more complex than indicated below. For example, although any VISA card issued outside of Brazil can be used inside Brazil and vice versa, there are three different varieties of VISA card within Brazil each of which may only be used within Brazil by merchants approved to take that VISA subtype...]

Since there is no standard code for Major International card brands (cards with numbers as defined in ISO xxxx), the following codes are adopted for use in UPP headers account-type bag field. Additional codes may be registered with IANA.

Code	Long Name
AX	American Express
DC	Diner's Club
DS	Discover
JB	Japan Bank Card
MC	MasterCard
VI	VISA