Internet Draft
Intended Status: Experimental
Expires: Feb., 2015

Shanghai Hongchuang WEB Technology Service Co., Ltd.
Tian Guorong
Shen Jun
Curtis Young
Oct. 10, 2014

HIEP: HTB Internet E-wallet Protocol
draft-tianguorong-hiep-02
This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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 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".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on Feb., 2015.

Abstract:
This document describes an online-paying method that realizes the paying addressing on the basis of HTTP protocol. It is for the purpose to setup a normative and safe E-paying system standard, and specify the definition of E-paying.

Table of Contents

1. Introduction

Till now, there's no one paying addressing language to realize the online paying or data set's interoperating that could be used for definite or name of E-currency's widely used. Under the promoting by W3C, the future generation WEB of the semantic web is defined as "the WEB concept structure which could be handled directly by the machine". On the background of this technology, this ID describes an E-currency paying public infrastructure of the bank pre-positive system in the field of e-paying.

1.1 Definitions

1) HTB㋡: the identifier of paying domain or paying address.

2) HIEP: HTB Internet E-wallet Protocol.

3) username: the name the E-wallet; xxxbank: to mark the field of the E-wallet

Field/

=domain name (xxx) ㋡

Root field abcbank.com/

=http://www.xxx㋡ xxxbank.com

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMENDED", "MAY", AND "OPTIONAL" in this document are to be interpreted as described in RFC-2119[RFC2119]. In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. HIEP Problem Statements

At present, differentiation of the payment communication and system structure are formed by independent bank organizations or 3rd party payment company's leading position, that they are using different payment models to describe the objects, and formulate each standard. Those standards just extend the life time of each existed systems, instead ensure the data exchange or dataset's interoperation between different paying systems. Obviously, it will restrict the application field online paying, and it could not reach the ability and technique of handling the paying activities of all kinds of bank cards.

The real-time of paying is finally a bottleneck problem of the E-business development. Without solving this problem, furthermore, it will bring the unsafe hidden trouble on the capital operation. For the time being, we can only say in own scope utmost, as it only can realize the online paying with safe within each own system. It cannot make the real-time online paying, and can not reach the comprehensive integration of huge scale (supranational, super-region, super-section).

Currency's credit: The currency is a credit symbol of paying, people trust it to make it as the intermediation of substitution. It is accepted by the social due to its characteristic advantage comparing the metal money on "Gold Standard System" or "Silver Standard System". Obviously, the symbol in virtual paying organizations transaction MUST use a unique identifier, which could make into a definition when people using. This is the credit problem in the paying procedure.

4. HIEP

This ID names and cites an unique ⓗ identifier to express the field which the user exists. The form is xxx (user) ⓗxxxbank.com. xxx(user) is the domain name, and xxxbank.com is the root field. On this basis, to resolve the xxx(user) ⓗxxxbank.com by http in order to setup the paying communication protocol for regulating E-currency activities form. Combining with html web, it could structure paying space data integrated service platform and be used to setup bank pre-positive e-paying system public infrastructure. A ⓗ paying communication protocol is http//www.xxxⓗxxxbank.com/,……

In order to avoid the complex of mis-operation by the web designer, it requires HTML and DOM API be designed into the ones which could not detect other script synchronous executing, even workers SHOULD obey this regulation with no exception. (Note: In this mode, navigator, yield for storage update() equal to turning back the calling for keeping other scripts executing.) On this base, the purpose of HIEP is to make the operation thought to be execution step by step the context paying scripts from the ⓗ ID in order to execute the HIEP termination's display data passing to the client ends smooth. The client ends here are PCs or non-PCs using different structure systems, i.e. the computers operating UNIX, Linux or DOS etc. Through the HIEP protocol, the computer could get the corresponding services from the remote operating server. Furthermore, it's structure supports multi point data transport, that could transfer to data from end server program to every client ends. i.e. Data are transported to multi destinations for synchronous execution from a real time application program.

Here, we would design an ⓗ e-wallet structure public account system supplying interface standard to connect with bank e-paying system, as it could interoperate the data between them.

4.1 General Design

4.2 System Module Division

4.3 ⓗ Paying Application

4.4 e-top Management Platform

5. HIEP Frame Format

5.1 HIEP Paying Protocol Description

5.1.1 HIEP Paying Net Definition

HIEP cites a (htb) as the unique identifier globally as the field of bank accounts for the seller and buyer. The format is user- -E.wallet bank, on the http.connection internet, the communication connect of the (htb) e-wallet is http://www.…….bank.com/. The is used as the only paying domain name or add. to realize that the users could make the paying transaction at anytime, anywhere, by any method, to any account.

HIEP Paying Net Technical Frame

HIEP consists of: domain name registration adm. organization, domain name global resolution service center, E-wallet paying transaction platform, HIEP Paying Net Account Settlement Center

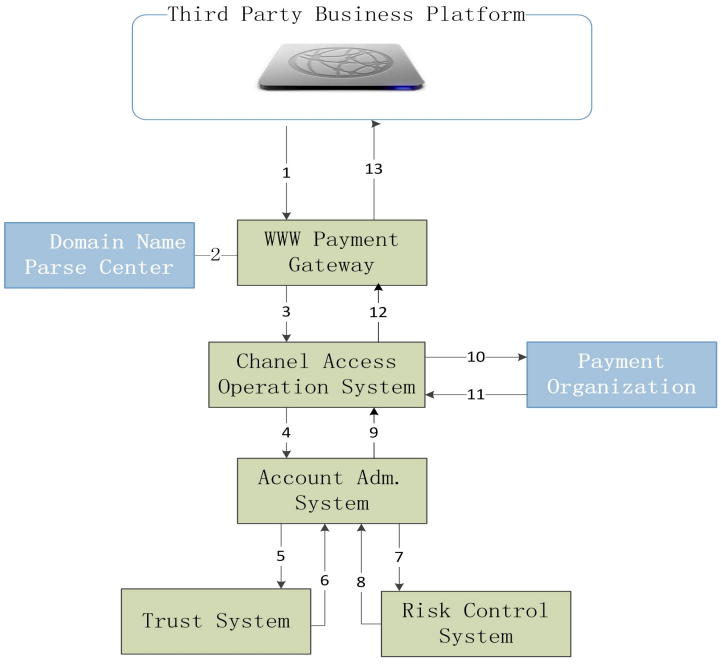
1. Domain Name Registration Adm. Organization: in charge of the domain name application response and domain information management maintenance.

2. Domain Name Global Resolution Service Center: take the responsibility of domain name resolution service. It will parse the name into the detail paying parameters including the bank account no., holder's relative financial information etc.

3. E-wallet Paying Transaction Platform: It carries all the 3rd business system accessing, the HIEP paying requests and dealing routes. It will pass all the HIEP paying requests from business onto the all the paying institutions which support the HIEP paying protocol standard.

4. HIEP Paying Net Account Settlement Center: It works to calculate and deal all the dealing data according to transaction records, and inform all the accessed the financial institutions to make the money settlement on time.

5.1.2 HIEP Transaction Flow chart:



Handling Procedure Description:

1.The 3rd business platform (i.e one merchant site) sent the paying request to HEIP www paying gateway.

2.www Gateway transmit the request to the ㊔ global resolution center to get the relative paying factors.

3.www Gateway transmit the requests to the channels accessing operation system.

4.The channel accessing operation system sends the related ㊔ account information to the account adm. System.

5.Account Adm. System sends the order data to the Trust System to check the trust data and information.

6.The Trust System returns the trust data to the Account Adm. System.

7.Account Adm. System sends the transaction data to the Risk Control System.

8.Risk Control System reverts with the risk treating result.

9.Account Adm. System processes the transaction data according to the HIEP regulations on the base of dealing result from Trust System and Risk Control System, and reverts the process result to the Channel Accessing Operation System.

10.Channel Accessing Operation System will pass the transaction requests routing to the related paying institutions (Banks or 3rd paying parties).

11.Paying Institutions revert the paying results.

12.Channel Accessing Operation System turns the paying results back the www paying gateway.

13.The www paying gateway inform the 3rd business platform with the transaction result.

5.1.3 Paying Mode Statement:

1.The individual user choose the commodity on the 3rd business platform to create an order.

2.The individual user send the paying request message to its own ㊔ domain name from the 3rd business platform after confirmation of the order. The send message is http html format, which includes the amount, ㊔ domain name of seller and buyer, commodity information, security certificate data, MAC verifying information etc.

3.The www paying gateway of HIEP responses on the requests, and resolve them into the HIEP protocol messages between the related financial institutions via HIEP's domain parse system and channels accessing operation system.

4.HIEP Paying Net reverts the paying request handling results from the financial institution to the request launcher's ㊔domain name (URL).

5.1.4 Transaction request message example:

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<HTML><!.㊔..bank.com=HTTP. ㊔㊔..!>

<Line string srs Name=http://openHICS.net/RBAC/srs/DRM.xml>

String.url=http://www... ㊔ ...bank.com/>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title> Single transaction consuming front stage display example</title>

</head>

<body>
<form action="abc" method="post">
<input type="hidden" name="account" value="abc㊋abc.com" alt="㊋ Account Field" />
<input type="hidden" name="bindid" value="㊋sss" alt="㊋ Account bounded ID, each ID should map to its account field. Only when the ID bounded to the account field, it could be used for transaction." />
<input type="hidden" name="biandpassword" value="㊋xxx" alt=" Each bounded ID should set a password, which is used to transaction. In order to satisfy some scenarios, the password is needed to deal the transaction between bounded ID and account field. " />
<input type="hidden" name="pid" value="" alt="Commodity No." />
<input type="hidden" name="pname" value="" alt="Commodity Name" />
<input type="hidden" name="price" value="" alt="Unit Price" />
<input type="hidden" name="amount" value="" alt="Quantity" />
<input type="hidden" name="busitype" value="" alt="Business Type" />
<input type="hidden" name="trantype" value="" alt="Deal Type" />
<input type="hidden" name="total" value="" alt="Total Amount" />
<input type="hidden" name="mid" value="" alt="Merchant No." />
<input type="hidden" name="bookid" value="" alt="Order NO." />
<input type="hidden" name="bookdate" value="" alt="Order Date" />
<input type="hidden" name="transdate" value="" alt="Order Time" />
<input type="hidden" name="currency" value="" alt="Currency" />
<input type="hidden" name="signtype" value="" alt="Signature Type" />
<input type="hidden" name="sign" value="" alt="Sign" />
<input type="hidden" name="country" value="" alt="Country ID" />
<input type="hidden" name="timezone" value="" alt="Time Zone" />
<input type="hidden" name="ip" value="" alt="IP Add." />
</form>
</body>
</html>

5.2 HIEP Paying Net Security & Authentication

5.2.1 Communication Security

Use encryption transmission for the key phrases (sensitive info as: card no., password, CVN, validity etc.) interaction with external systems.

5.2.2 Data Security

Password Protection System

Using different algorithms for the users logging and account passwords which saves in the system database.

5.2.3 Data Communication Security

In order to avoid tampering with the data, the communication data needs to increase the verifying fields.

5.2.4 External Systems

Use RSA sign algorithms for those key data fields.

5.2.5 Internal Systems

Use DES CBC to create the abstract.

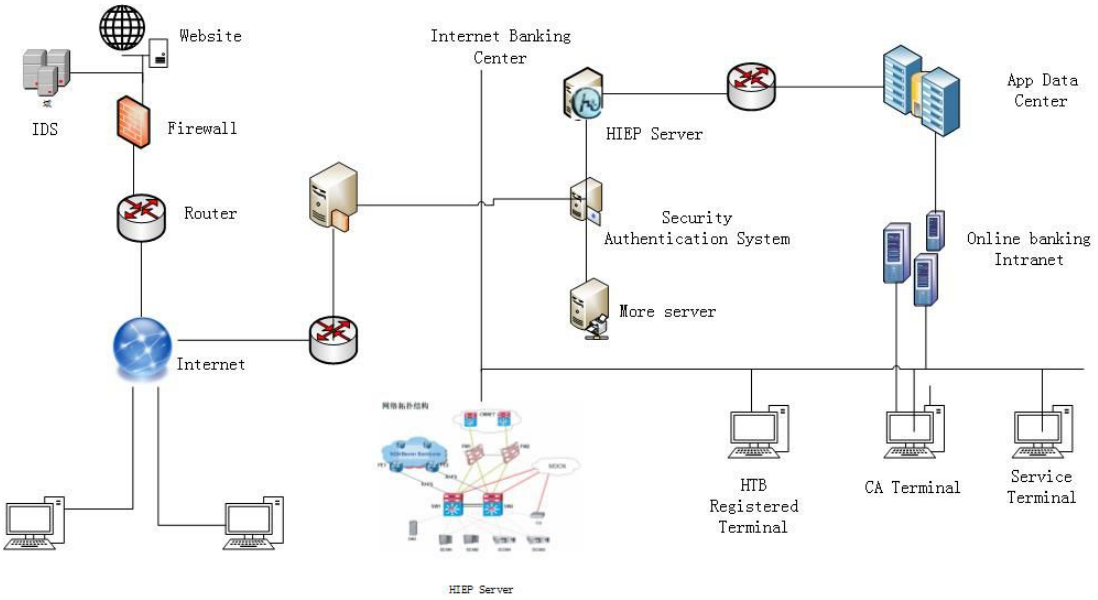
5.2.6 Date Storage Security

All the saved account and ID no. etc. should be encrypted to avoid the embezzlement.

6.HIEP Deployment Scenarios

6.1 The WEB structure from HIEP system

6.2 The commercial bank net structure on the base of HIEP



6.3 HIEP Paying Modes comparing with the existed types of paying modes

图2.1 Bank Paying Gateway Mode

图2.2 Online Bank Paying Mode

图2.3 Uniform Paying Gaterway Mode

图2.4 3rd Party Paying Gateway

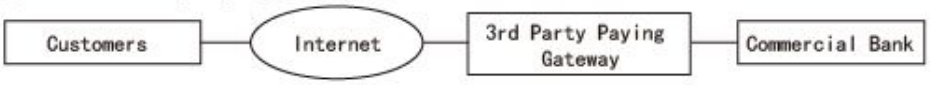
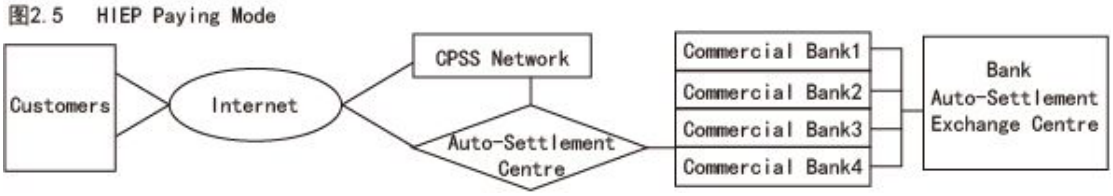


图2.5 HIEP Paying Mode



7. Security Considerations

In order to realize the interconnection and mutual certification, the HIEP mutual information approval is refer to X.509V3 extension. It is merged into PKCS#12, the indicated HTB domain name MUST be the first level domain name of a bank. Bind the user's public key information with other identified information including the username and email add., to complete the certification of users on the internet.

8.IANA Considerations

The IANA will configure the HTB port for HIEP.

9.Conclusions

This document describes the pre-position E-currency paying public infrastructure of bank in the field of the internet E-paying, that realize the HIEP on the HTTP protocol according to the open standard of W3C.

10.References:

[RFC2119] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[RFC2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol - HTTP/1.1", June 1999

[RFC1866] T. Berners-Lee, D. Connolly, "Hypertext Markup Language - 2.0", November 1995

Author's Address:
Tian Guorong
Shanghai Hongchuang WEB Technology Service Co., Ltd.
Bldg 14, Xinyun Economic Zone, Lane 3199 Zhenbei Rd.
Shanghai, China
Phone no.: 0086 135 8592 1617
Email: bill.tian@shcn.cc

Shen Jun
Phone No.: 0086 133 0171 0551
Email: jun.shen@shcn.cc

Curtis Yang
Phone No.: 0086 138 0178 0703
Email: curtis.yang@shcn.cc