Hosted Payment Capture Systems Specification

Version 1.0

11 May 2012

About HTNG

Hotel Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century; to be recognized as a leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community; and to facilitate the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed.

The names Hotel Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hotel Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hotel Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.

Table of contents

1 This Specification at a Glance

A Hosted Payment Capture System provides the means to collect payment information from a customer on a system that is hosted by someone other than the hotelier, therefore reducing the number of hotel systems within the scope of PCI. Many hotel companies find the need to use the resources of multiple payment capture systems in the course of their business. This specification addresses this need by creating a standard for interaction between these Hosted Payment Capture Systems and the hotel.

There are no new message definitions encompassed within this specification. Rather, this specification details the implementation standard for Hosted Payment Capture Systems and leverages the existing messages from the current HTNG Payment Systems & Data Security specifications: the Payment Processing specification and the Data Proxy specification. It also defines the roles for such an implementation.

2 Document Information

2.1 Document History

Version	Date	Author	Comments
0.01	15 Nov 2011	Kevin Doucette	Initial Use Cases
0.02	16 Nov 2011	John Bell	Initial Use Cases
0.03	24 Feb 2012	Brian Alessi	Section 1 & 2 Draft
0.04	12 Mar 2012	Brian Alessi and John Bell	Updated references to Payments specification; updated use cases
0.05	20 Mar 2012	John Bell	Updated use cases and Implementation Notes
0.06	21 Mar 2012	Jay Rosamilia	Updated Use Cases, inserted diagrams, general formatting.
0.07	21Mar 2012	Kylene Reese	Updated general formatting of the spec
0.08	29 Mar 2012	HPCS Workgroup	Deleted use cases and updated roles
0.09	10 Apr 2012	Jay Rosamilia	Updated diagrams and created sample messages.
0.10	11 Apr 2012	Jay Rosamilia	Added redirected web form example
0.90	13 Apr 2012	Kylene Reese	Member review period
0.91	4 May 2012	Kylene Reese	Vote period
1.0	11 May 2012	Hosted Payment Capture Systems Workgroup	2012A Release

2.2 Document Purpose

The purpose of this document is to provide an implementation specification, which uses HTNG open standards solutions for Hosted Payment Capture Systems. It also serves as a specification for defining the roles of the Hosted Payment Capture System.

2.3 Scope

The scope of this document includes implementation for secure transactions over the Web. With Web transactions, a content proxy is defined as a use case, as well to facilitate the role of the Hosted Payment Capture System.

2.4 Relationship to Other Standards

This specification will leverage existing HTNG open standards specifications such as the Payment Systems & Data Security Payment Processing specification and the Payment Systems & Data Security Data Proxy specification, as well as existing secure data transfer standards such as FTP-Secure and WebDav.

2.5 Audience

The primary intended audience of this document is a developer or system designer seeking to implement the interface specifications within their products. As this document also provides Business Level Use Cases, the secondary audience is general business readers wishing to familiarize themselves with the interactions between POS, Gateways and Hosted Payment Capture Systems.

2.6 Overview

The existing Payment Systems & Data Security Payment Processing specification and Payment Systems & Data Security Data Proxy specification can be leveraged to illustrate how the below component scenarios interface with the Hosted Payment Capture System. This includes messages for placing a new reservation and a new reservation with a deposit. These messages (or set of messages) currently exist within the Payment Systems & Data Security specifications. More importantly, it is the role of the Hosted Payment System, Hotel content Publisher and Hotel Web Site which we define. Concerning web-based transactions, this specification details how content is transferred between the Hotel Web Site and the Hosted Payment System.

2.7 Known Limitations

No known limitations.

3 Component Scenarios

3.1 Web-Based Reservation or Payment, No Card on File

3.1.1 Overview

A customer wishes to reserve or pre-pay for a room or make a purchase using a hotelier provided web-site. The hotelier does not have a payment token associated with the customer on file.

3.1.2 Roles

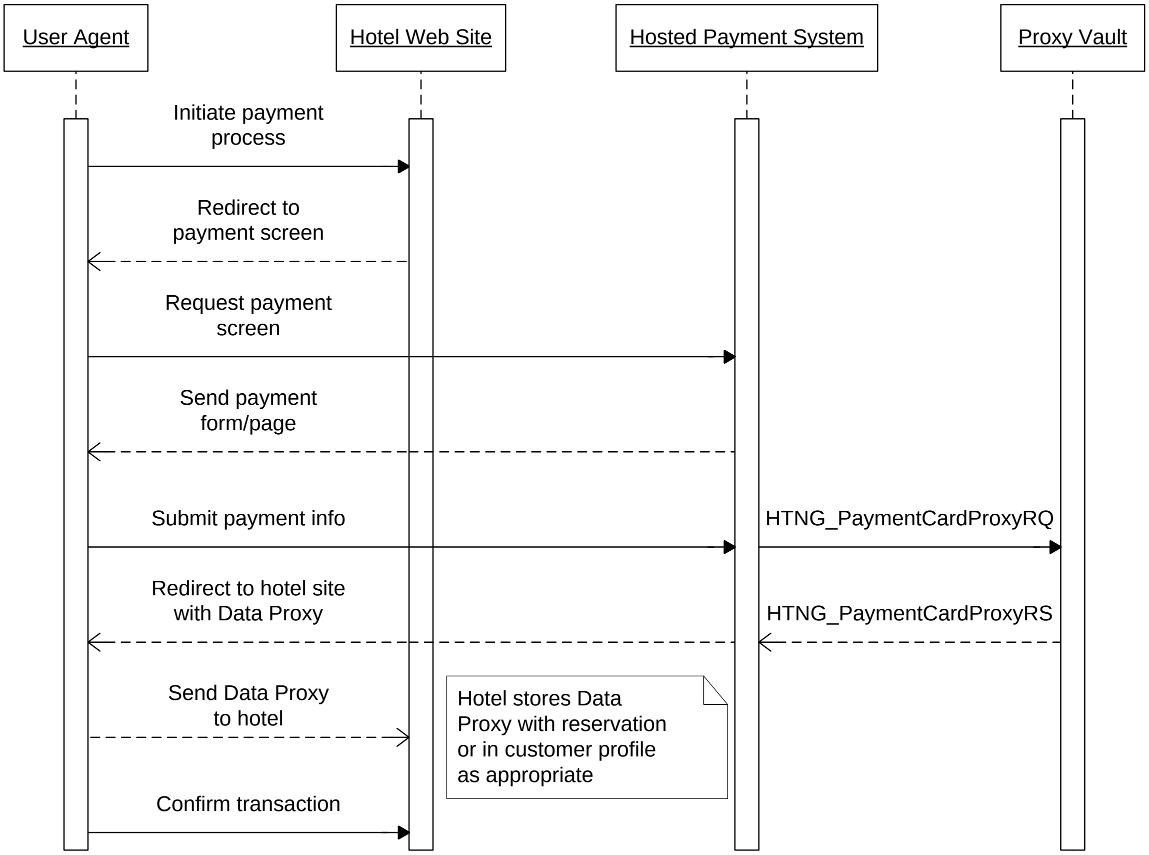
User Agent	Browser or application directed by the customer to complete a transaction on their behalf
Hotel Web Site	The web site provided by the hotelier
Hosted Payment System	The system that presents a web page where payment information is securely collected
Proxy Vault	A secure system that stores sensitive data in a secure manner, preferably in an encrypted form

3.1.3 Use Case

Use Case Name:	**Web-based Reservation or Payment, No card on file**
Summary:	The customer wishes to: • Make a reservation on the hotel web site and needs to guarantee the rooms with a credit card, or • Make a reservation on the hotel web site for a room that requires pre-payment, or • Purchase merchandise or other amenities that require payment. There is no card on file for the customer so credit card data must be collected.
Basic Course of Events:	1. Customer follows link to add credit card information. 2. Hotel Web Site sends customer to Hosted Payment System. 3. The Hosted Payment System sends HTNG_PaymentCardProxyRQ (4.1 in the Payment Systems & Data Security Data Proxy Specification) to the Proxy Vault and will receive HTNG_PaymentCardProxyRS (4.2 in the Payment Systems & Data Security Data Proxy Specification) in return. 4. Hosted Payment System redirects customer back to Hotel Web Site with data proxy stored in a hidden HTML form. 5. Browser follows redirect, giving data proxy to Hotel Web Site. 6. Hotel can process payment as needed – issues an

	HTNG_PaymentCardProcessingRQ (with the TransactionType set to Sale) to the Payment Processing System and will receive an HTNG_PaymentCardProcessingRS (6.1.2 of Payment Systems & Data Security Payment Processing specification) in return
Exception Path:	
Alternative Paths:	
Trigger:	
Assumptions:	
Preconditions:	No data proxy is on file with the hotel
Postconditions:	Hotel has data proxy that can be charged later as necessary

3.1.4 Message Flows



3.1.5 Sample Request

```
<HTNG_PaymentCardProxyRQ EchoToken="9bae1a5f-c8fc-47ad-b257-3eb035ce9d81" PrimaryLangID="en-us"
RetransmissionIndicator="false" SequenceNmbr="12345689" Target="Test" TimeStamp="2012-03-
30T17:47:20.563-05:00" Version="2.0">
        <POS>
                <Source>
                        <RequestorID ID="HTNG" ID_Context="HTNG" Type="16">
                                <CompanyName Code="HTNG" CompanyShortName="Hotel Technology Next
Generation"/>
                        </RequestorID>
                </Source>
        </POS>
        <PaymentCards>
                <PaymentCard CardCode="VI" CardNumber="4444333322221111" ExpireDate="1216">
                        <CardHolderName>Aanson B Campbell</CardHolderName>
                </PaymentCard>
        </PaymentCards>
</HTNG_PaymentCardProxyRQ>
```

3.1.6 Sample Response

```
<HTNG_PaymentCardProxyRS EchoToken="9bae1a5f-c8fc-47ad-b257-3eb035ce9d81" PrimaryLangID="en-us"
RetransmissionIndicator="false" SequenceNmbr="12345689" Target="Test" TimeStamp="2012-03-
31T11:09:17.056-05:00" Version="2.0">
        <Success/>
        <ProxyIDs>
                <ProxyID>4802432714031111</ProxyID>
        </ProxyIDs>
</HTNG_PaymentCardProxyRS>
```

3.1.7 Sample Redirect

The following shows how the Hosted Payment System can leverage the User Agent to act as pass-through (via a forced redirect) to provide values to the Hotel Web Site.

```
<!DOCTYPE HTML>
<html>
    <head>
        <title></title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    </head>
    <body onload="document.forms['theForm'].submit()">
        <form id="theForm" action="receiveProxy.jsp" method="post">
            <input type="hidden" name="ProxyID" value="aaaabbbbccccdddd5"/>
            <input type="hidden" name="CardCode" value="VI"/>
            <input type="hidden" name="MaskedCardNumber" value="XXXXXXXXXXXX1111"/>
            <input type="hidden" name="ExpireDate" value="0115"/>
            <input type="hidden" name="OptionalField1"
value="HMAC_MD5:0x74e6f7298a9c2d168935f58c001bad88"/>
        </form>
    </body>
</html>
```

3.2 Content Push

3.2.1 Overview

The Web Pages served by the Hosted Payment System need to have the same look and feel as the Hotel Web Site, but the hotel company needs to be able to quickly modify the appearance of their site to meet their business needs. This must be done without compromising the security of the Web Pages used to collect payment information from the customer. One solution to this is for the Hotel to provide content templates with markers that allow the Hosted Payment System to merge the content with the web forms required to collect payment information.

The Content Templates consisting of HTML files, style sheets, and images need to be stored on the Hosted Payment System resources. The Hosted Payment System provides secure access for the Hotel Content Publisher to update the Content Templates when the content changes. This access is provided by standard tools and protocols like secure FTP or WebDav.

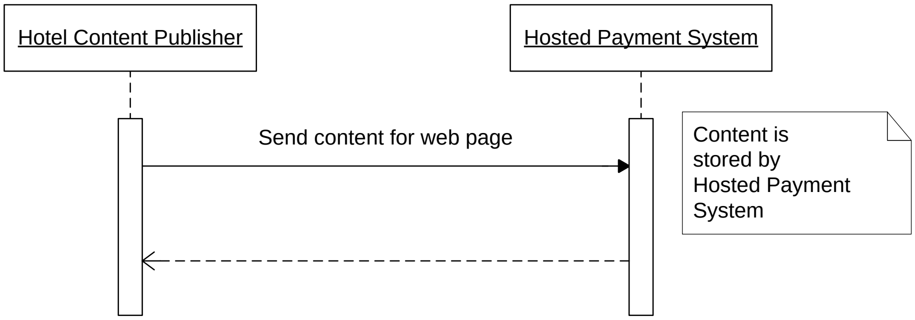
3.2.2 Roles

Hotel Content Publisher	Publishes Content Templates to the Hosted Payment System to match web site look and feel
Hosted Payment System	The system that presents a web page where payment information is securely collected; this system also provides a place to store Hotel provided Content Templates

3.2.3 Use Case

Use Case Name:	**Content Push**
Summary:	The Hotel wants to provide or update the Hotel content on the payment page. Content includes HTML, CSS, and images. The Hosted Payment System provides a secure storage location for the content.
Basic Course of Events:	Note: In this use case, it is recommended to use a standard existing protocol like Secure FTP or WebDav. 1. For each file to be deleted, the Hotel Content Publisher deletes file from Hosted Payment System. 2. For each file to be added or update, the Hotel Content Publisher copies file to Hosted Payment System.
Exception Path:	
Alternative Paths:	
Trigger:	
Assumptions:	
Preconditions:	• The Hotel Content Publisher has Content Templates ready to publish. • The Hosted Payment System has storage capability. • The Hotel Content Publisher has secure access to the Hosted Payment System to manage (add, update, delete) Content Templates.
Postconditions:	• Content Template is deployed to Hosted Payment System.

3.2.4 Message Flows


Hotel Content Publisher
Hosted Payment System
Send content for web page
Content is stored by Hosted Payment System

3.2.5 Sample Request

Not applicable – recommend use of secure FTP or WebDav protocols.

3.2.6 Sample Response

Not applicable – recommend use of secure FTP or WebDav protocols.

3.3 Content Pull (Content Proxy)

3.3.1 Overview

The Web Pages served by the Hosted Payment System need to have the same look and feel as the Hotel Web Site, but the Hotel needs to be able to quickly modify the appearance of their site to meet their needs. This must be done without compromising the security of the pages used to collect payment information from the customer.

Acting as a content proxy, the Hosted Payment System retrieves and caches Content Templates from the Hotel Web Site and merges the Content Templates with the web forms required to collect payment information.

3.3.2 Roles

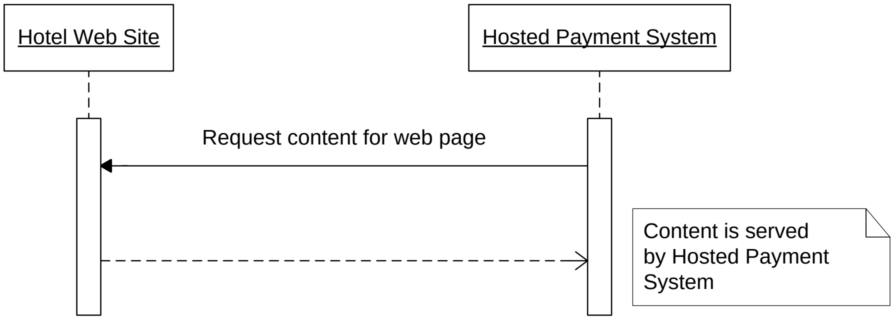
Hotel Web Site	The web site provided by the hotelier
Hosted Payment System	The system that presents a web page where payment information is securely collected

3.3.3 Use Case

Use Case Name	**Content Pull (Content Proxy)**
Summary:	The Hosted Payment System needs to update the Content Template provided by Hotel. The Hotel Web Site hosts common content on its own servers. The Hosted Payment System retrieves the Content Template from the Hotel Web Site and merges it with its own web forms.
Basic Course of Events:	1. Hosted Payment System uses HTTPS to request Content Template.

	2. Hosted Payment System merges Content Template with its web forms. 3. Hosted Payment System remaps links embedded in Content Template to point to Hosted Payment System. 4. Hosted Payment System retrieves and caches resources referenced in Content Template from Hotel Web Site.
Exception Path:	
Alternative Paths:	
Trigger:	
Assumptions:	
Preconditions:	• The Hotel has Content Template ready and hosted on Hotel Web Site. • Hosted Payment System has URL for the Content Template.
Postconditions:	• Content Template is merged with Hosted Payment System web forms and sent to browser.

3.3.4 Message Flows


Hotel Web Site
Hosted Payment System
Request content for web page
Content is served by Hosted Payment System

3.3.5 Sample Request

The request is a standard HTTP request for the HTML base document and subsequent requests for the CSS and images.

3.3.6 Sample Response

The response is a standard HTTP response returning the HTML, CSS, or image as requested.

4 Appendices

4.1 Glossary of Terms

For the purpose of this document the following terms have been defined as follows:

Term	Definition
Content Template	Consists of HTML cascading style sheets and JavaScript with markers that can be used to merge other information into the template to create a web page
Hosted Payment System	The system that presents a web page where payment information is securely collected; this system also provides a place to store Hotel provided Content Templates
Hotel Content Publisher	Publishes Content Templates to the Hosted Payment System to match web site look and feel
Hotel Web Site	The web site provided by the hotelier
Proxy Vault	A secure system that stores sensitive data in a secure manner, preferably in an encrypted form
User Agent	Browser or application directed by the customer to complete a transaction on their behalf

4.2 Implementation Notes

This specification is based on the Payment Systems & Data Security Payment Processing Specification 2010B version 2.0 and the Payment Systems & Data Security Data Proxy specification version 1.1. This Hosted Payment Capture Systems specification was written when the above versions were the most recent of the specifications. Please note that if new versions of the existing specifications are created, the referenced use cases may not match exactly.

4.2.1 Security Considerations

In order to avoid Cross Frame Scripting and Click Jacking attacks, IFrames should not be used (see: https://www.owasp.org/index.php/Cross_Frame_Scripting and https://www.owasp.org/index.php/Clickjacking). The best way to mitigate the danger from these attacks is to avoid the use of Frames and remove any active Frames that may be in use. This means that IFrames should not be used to deliver content from the Hotel site that load a payment frame. By not allowing frames and serving all of the content from the Hosted Payment System, the JavaScript is limited to the sandbox of the Hosted Payment System.

4.2.2 Sample Hotel Content

The content shown in the example below is an example of content that might be provided by the Hotel. The Hosted Payment System merges the form by looking for the <div> with the id set to “PaymentForm” and setting the contents of the block to the payment form content, or by replacing the string “{PaymentForm}” with the form content.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<!-- Example of possible hotel content -->
<html>
 <head>
  <title>Generic Hotel Payment Form Example</title>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <style type="text/css">
   #PaymentForm p {color:red}
    #PaymentForm label {color:red}
   </style>
  </head>
  <body>
   <h1>Generic Hotel Page</h1>
   <p>This content is provided by the hotel</p>
   <div id="PaymentForm">{PaymentForm}</div>
   <p>This content is provided by the hotel</p>
   <script type="text/javascript">window.onload=GetForm();</script>
  </body>
 </html>
```

4.2.3 Sample Hosted Provider Form

The content shown below is a simplified representation of a payment form than might be inserted into the hotel provided content as shown above.

```
<form action="PostPayment" method="POST">
  <p>This content comes from the payment service provider</p>
  <p><label>
   Name:<input type="text" name="name" value="your name" />
  </label></p>
  <p><label>
   Expires:<input type="text" name="expires" value="some date" />
  </label></p>
  <input name="ok" type="submit" value="OK" />
   <input name="cancel" type="submit" value="Cancel" />
   <p>This content comes from the payment service provider</p>
 </form>
```

4.2.4 Sample Merge Code

The JavaScript snippet below shows one possible way to merge the form into the hotel content.

```
<script type="text/javascript">
 function GetForm(){
  xmlhttp = new XMLHttpRequest();
  xmlhttp.open("GET","PaymentForm.html",false);
  xmlhttp.send();
  document.getElementById("PaymentForm").innerHTML=xmlhttp.responseText;
 }
</script>
```

4.3 Referenced Documents

The following table shows the documents upon which this document depends:

Document Title	Location/URL
Payment Systems & Data Security Payment Processing Specification	http://collaboration.htng.org/specs/documents.php?action=show&dcat=34&gdid=23080
Payment Systems & Data Security Data Proxy specification	http://collaboration.htng.org/specs/documents.php?action=show&dcat=32&gdid=22006