Facilitated Transaction Checkout Web Service Specification

FINAL DRAFT – Version 1.1
December 17, 2003

NPCC Control Areas
- NYISO
- ISO-NE
- Hydro Quebec TransEnergie
- IMO, Ontario
- New Brunswick Power

Contact Information:
- Phil Phoenix (NYISO) at 518-356-6000
- Fred Theadore (NYISO) at 518-356-6000
- Mike Martin (NYISO) at 518-356-6000

Table of Contents

1 Introduction

The Facilitated Checkout Web Service is a standards-based technology for exchange of transaction checkout data between Control Areas.

1.1 Purpose

This specification details a Web Service that can be implemented to enable Facilitated Checkout. Continued collaboration among NPCC members will evolve this specification. The Facilitated Checkout Web Service can be implemented with any Web Services compliant technologies including J2EE and Microsoft based products. Adherence to this specification guarantees interoperability regardless of technology platform.

1.2 Audience

This specification is intended to provide sufficient technical detail and business context to allow technologists to design and deploy the Facilitated Checkout Web Service. Readers are presumed to be familiar with the terms in the Internet Security Glossary.

1.3 Notational Conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119.

Namespace URIs (of the general form "some-URI") represent some application-dependent or context-dependent URI as defined in RFC2396.

2 Web Service Definition

Web Service Description Language [WSDL] is used to describe the technical details of each message and operation defined the Facilitated Checkout Web Service.

The WSDL for a Web Service exists in two forms. The abstract form details the structure of the Web Service in the form of messages and operations. The WSDL can also exist in a concrete form. A concrete WSDL includes all definitions within the abstract WSDL as well as specific URL endpoints and communication protocol. The focus of this specification is the abstract definition of the Web Service to ensure interoperability. Concrete aspects of the WSDL will differ among control areas.

The Facilitated Checkout utilizes the document / literal messaging strategy to increase platform compatibility.

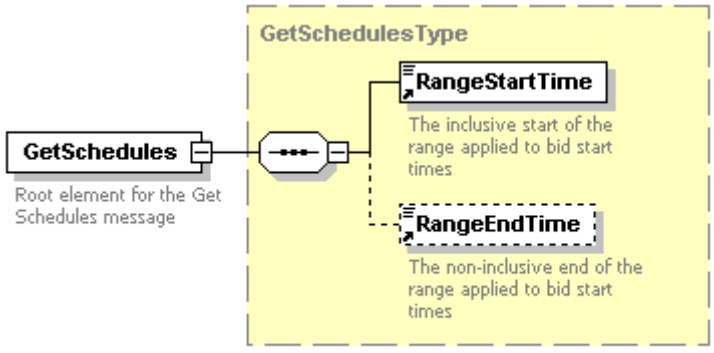
For optimum compatibility the WSDL MUST conform to the WS-I Basic Profile 1.0. The WSDL SHOULD be validated by the WS-I Implementation Tool. However, the current release of the implementation tool does not contain the full set of test assertions. Therefore, output from the tool cannot be used to make any statements about WS-I conformance.

2.1 Messages

The Facilitated Checkout Web Service defines two input messages. The Get Schedules Message is used to retrieve schedules for a specified time range. The Schedule Available Message notifies the receiver that new or updated schedule information is available.

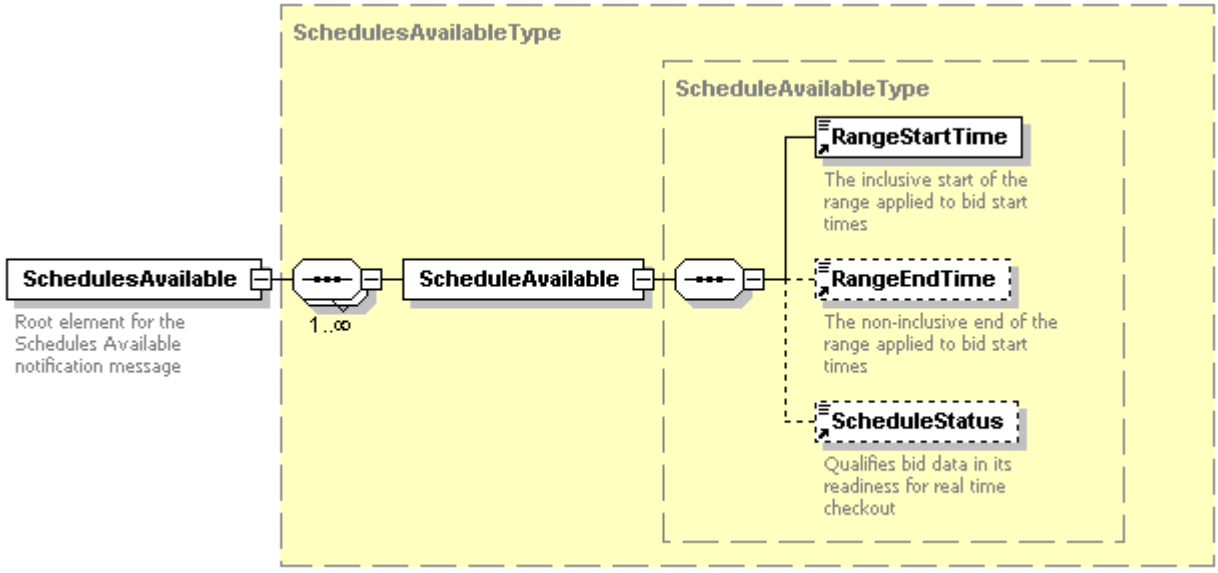
2.1.1 Get Schedules Message

The Get Schedule Message is used to request a range of bid schedules. This message is the input for the Get Schedules Operation.



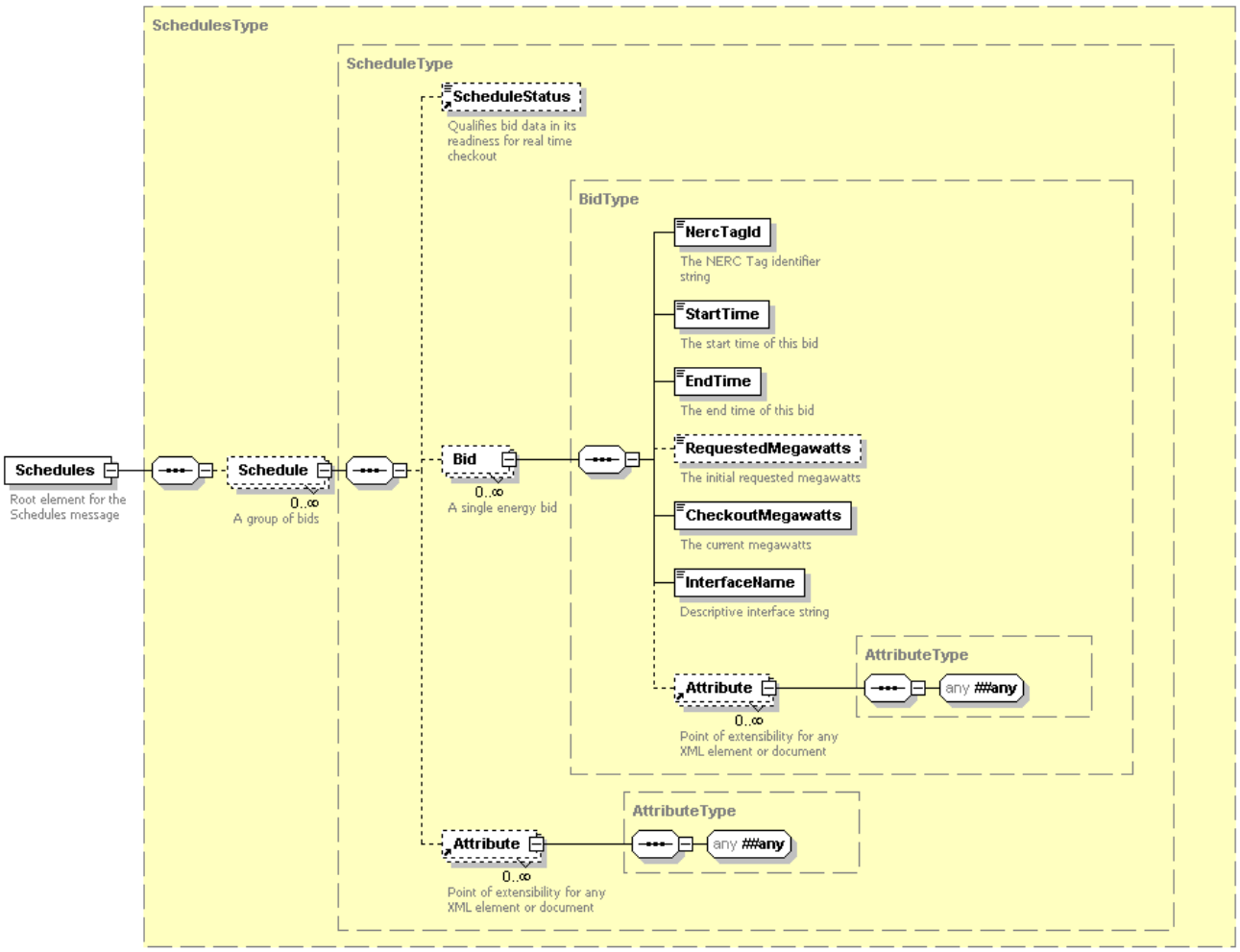
2.1.2 Schedules Available Message

The Schedule Available Message is used to communicate a newly available or modified data set. This message is the input for the Schedules Available Operation.



2.1.3 Schedules Message

The Schedules Message is returned from successful invocations of the Get Schedules Operation.



2.2 Element Descriptions

2.2.1 Global Element: RangeStartTime

The RangeStartTime element reflects the earliest start time of all bids within a range of bids. This element is a child of the GetSchedules element and the ScheduleAvailable element.

Within the GetSchedules:
This element represents the earliest bid start time in the range. Results will have a start time no earlier than the specified time.

Within ScheduleAvailable:

This element represents the earliest start time of bids in the described range.

2.2.2 Global Element: RangeEndTime

The RangeEndTime element qualifies a range of bids as having start times earlier than this value. This element is a child element within GetSchedules and ScheduleAvailable.

Within GetSchedules:
RangeEndTime limits the scope of the request to a range of bids that have a start time earlier than this value.

Within ScheduleAvailable:
RangeEndTime describes the range of bids as having start times earlier than this value.
.

2.2.3 Global Element: ScheduleStatus

The ScheduleStatus element is OPTIONAL. Implementations that do not support this element MUST omit the element. If the element is included it MUST NOT be empty. Valid values are 'Preliminary' and 'CheckoutReady'.

The ScheduleStatus element denotes the readiness of bid data for real time checkout. Control areas that have a regular detectable event that renders a set of bids ready for checkout MAY implement this element. If implemented, the status MUST be 'Preliminary' before the event occurs and 'CheckOutReady' after the event occurs.

Value	Description
Preliminary	This data represents the best available data at this time. Data MAY change before the real time checkout begins.
CheckoutReady	This data represents the best available data at this time. Data is not expected to change before real time checkout begins.

2.2.4 Global Element: Attribute

Attributes describe aspects of Bids that further enhance the checkout process. Each Attribute element can contain an XML document of any type or schema. The document may be a single element. The content processing of the Attribute element is set to 'lax'. Therefore, unknown schema and types will not impact document validation. Conversely, known schemas can be validated and parsed as XML documents.

Control Area Specific Information
It is expected that control areas will define schemas that represent information particular to their information base.

Common Information

Control areas should collaborate with other control areas to define schema for shared information sets.

Schemas should be distributed to all consumers of the web service. Attribute schemas are detailed in the Attribute Implementations section.

Within Schedule:
Information within the Attribute applies to all bids of this schedule.

Within Bid:
Information within the Attribute applies to this bid only.

2.2.5 Element: Schedules

The Schedules element is the root element for the Schedules Message. It may contain zero or more Schedule elements.

2.2.6 Element: Schedule

The Schedule element provides a mechanism for grouping bids that MAY have common attributes. Element ScheduleStatus MAY be specified.

2.2.7 Element: Bid

The Bid element represents a single energy bid. It contains required elements NercTagId, StartTime, EndTime, RequestedMegawatts, CheckoutMegawatts, and InterfaceName.

2.2.8 Element: NercTagId

The NercTagId element is the string representation of the NERC tag identifier.

2.2.9 Element: StartTime

The StartTime element is the time at which the energy bid starts.

2.2.10 Element: EndTime

The EndTime element is the time at which the energy bid ends.

2.2.11 Element: RequestedMegawatts

The RequestedMegawatts element represents the initial requested megawatts of the bid. This element is OPTIONAL. Sign convention on Megawatt values are provided from the reference of the data provider. Sign MUST be defined as follows:

- Exports of the data providing control area will have a **positive** sign.
- Imports of the data providing control area will have a **negative** sign.

2.2.12 Element: CheckoutMegawatts

The CheckoutMegawatts element represents the current scheduled megawatts. This value may change during the checkout process. Sign MUST be defined as follows:

- Exports of the data providing control area will have a **positive** sign.
- Imports of the data providing control area will have a **negative** sign.

2.2.13 Element: InterfaceName

The InterfaceName element is OPTIONAL. Each service implementation MAY provide InterfaceName as they define it and as currently agreed to and utilized by neighboring Control Areas.

2.3 Web Service Operations

2.3.1 Get Schedules Operation

Providers of the Facilitated Checkout Service MUST implement the Get Schedules Web Service operation. Data returned from this operation is constrained according to the definitions of the Get Schedules Message. The get schedules operation MUST provide data visibility that correlates and supports the real time checkout process.

2.3.2 Schedules Available Operation

Implementations of the Facilitated Checkout Service MAY implement the Schedules Available Operation. This operation provides a method of notification that can be invoked from other control areas. Implementations of the Notification Process will invoke this operation.

3 Notification Process

The notification process is the invocation of the Schedules Available Operation on of other control areas when a significant change in the status of a set of bids occurs. Implementations of the Facilitated Checkout Service MAY implement the notification process. Implementations of the Notification Process SHOULD notify neighboring control areas that have implemented the Schedules Available Operation.

4 Attribute Implementations

4.1 Schedule Attributes

Schema Namespace	http://www.nyiso.com/2003/checkout-attributes		
Root Element	Provided	Providing Control Area	Utilizing Control Areas
LocalMarketType	Always	NYISO	ISO-NE

Schema Namespace			
Root Element	Provided	Providing Control Area	Utilizing Control Areas

4.2 Bid Attributes

Schema Namespace			
Root Element	Provided	Providing Control Area	Utilizing Control Areas

5 Data Visibility

The get schedules operation MUST provide data visibility that correlates and supports the real time checkout process. The operation MAY provide additional data visibility. The following table describes data visibility as implemented by various control areas.

Control Area	Data Visibility
ISO-NE	Scheduling algorithm executed at about –45 of the hour.
NYIS	CheckoutReady from –45 to 0; LocalMarketType: HAM Post Preliminary from –105 to –45; LocalMarketType: HAM Advisory Preliminary from DAM posting to –105; LocalMarketType: DAM Post Note: DAM Post not yet available

6 Security

A common security methodology will allow simpler integration of multiple control area Web Services. To this end, this specification will RECOMMEND a security model for Facilitated Checkout Web Services. However, we do not expect that each Control Area will have at its disposal the same security infrastructure. In any event, each Control Area must understand the security risk inherent in their implementation, and in a Memorandum of Understanding agree to a responsibility to treat this information as highly confidential.

6.1 Goals

Secure Web applications require a mechanism to support confidentiality, authentication, integrity and non-repudiation. Soon NERC will facilitate this mechanism through NERC-certified "Energy Market Access and Reliability" (e-MARC) certificates as described in an industry certificate policy (see reference 10).

Our goal is to anticipate the use of the e-MARC Policy, but not to the extent that it delays implementation.

6.2 Recommendation

It is recommended that the Facilitated Checkout Web Service utilize SSL over HTTP. SSL can use certificates bi-directionally. Server Certificates are sent to clients to validate the identity of the server to the client. Client certificates are sent to the server to validate the identity of the client to the server. This form of bi-directional transport layer identity validation is RECOMMENDED.

Item	Description	Purpose
1	SSL Server Certificate	Sent to client to allow client to validate identity of server.
2	SSL Client Certificate	Sent to the server to allow server to validate identity of client.
3	Certificate Authority (CA) Certificate	Used to sign Server and Client Certificates

To enable server identity validation, Control Area centers must configure trust of the CA certificate (Item 3) that was used to sign the neighboring Control Area's server certificate (Item 1). Adding the CA certificate to the root certificate store accomplishes this. This must be done before any exchange of any type of SSL.

Servers initiating SSL sessions with other servers outside the center's network should present a client certificate (Item 2) for authentication. This is called authenticated or two-way SSL.

e-MARC will employ certificates that follow the X.509 Version 3 (v3) standard. Facilitated Checkout should adopt this certificate type.[1]

Control Area centers MAY elect to employ an additional layer of security with HTTP Basic Authentication. Due to the established SSL connection, principles and credentials are encrypted as they travel to the server. Clients of these services need only to set the appropriate principle and credential (username and password) according to HTTP header specification.

6.2.1 Authentication

A Control Area may require a client certificate signed by a Certificate Authority (CA), such as OATI or GeoTrust. In this case, the Control Area should provide the automated means for a client certificate to be authenticated at the Control Area center's authentication server.

For the early stages of this project the distinguished name requirements in the NERC Policy will not be adopted, since currently Control Areas require different extensions to certificate contents. This means a single certificate per user across all Control Areas cannot be adopted.

6.2.2 Authorization

Facilitated Checkout Web Services requires that a user be authorized. When a server as client initiates a session, there must be a means to restrict data access based on identity.

With a client certificate (Item 2), the user name or identifier can be part of its contents and used for authorization. Each Control Area center may require different details in fields in the certificate's distinguished name that are tied to its present implementation of security authorization.[2]

Each Control Area will have to provide the automated means for a client to be authorized at the application and/or at the Control Area center's authentication server.

6.3 Scenarios

The following authentication / authorization scenarios are included for Web Services implementation.

6.3.1 ISO New England

ISO New England requires that an onsite-issued GeoTrust client certificate signed by the GeoTrust CA root be authenticated and authorized at the Control Area center's single sign-on server for all Internet business traffic into the enterprise network. The public key for each user is matched in a lookup table containing registered authorizations to the various market applications.

[1] Note: Also in the NERC Policy a certificate issued for a device or application is distinguished from a user certificate, and this is not in present implementations.

[2] For example ISO New England uses a certificate wherein the subject field OU identifier must contain User Id - NNNNN to authorize a unique user across its market applications.

Once the user is authorized to use the application, the user is redirected to the Facilitated Checkout application server where further authorization to determine the data content for the user's organization is done. The application server accesses the database associated with external transactions, which contains users and organizations, for final authorization.

7 Service Level Agreements

A service level agreement is an agreement regarding the guarantees of a web service. It defines mutual understandings and expectations of a service between the service providers and service consumers. The service guarantees are about what transactions need to be executed and how well they should be executed. [Li-jie Jin]

While the scope of this specification does not encompass specific service level agreements, it is RECOMMENDED that service levels be formally addressed. It is expected that agreements between individual parties will be formed.

8 References

1. Notations, http://www.ietf.org/rfc/rfc2119.txt
2. Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt
3. URI, http://www.ietf.org/rfc/rfc2396.txt
4. Web Services Interoperability Organization, www.ws-i.org
5. WSI Basic Profile 1.0, http://www.ws-i.org/Profiles/Basic/2003-08/BasicProfile-1.0a.htm
6. WSI Basic Profile Testing Tools, http://www.ws-i.org/implementation.aspx
7. Web Services, http://www.w3.org/2002/ws/
8. WSDL, http://www.w3.org/TR/wsdl
9. Analysis on Service Level Agreement of Web Services, Li-jie Jin, Vijay Machiraju, Akhil Sahai, http://www.hpl.hp.com/techreports/2002/HPL-2002-180.pdf
10. Certificate Policy for Energy Market Access and Reliability Certificates (e-MARC), Version 2.0, August 2003.