Exchange Network and Node Overview

Prepared for the Exchange Network Knowledge Transfer Meetings
Chicago, Illinois - April 22, 2003
San Francisco, California - May 5, 2003
What Is a Network Node?

- A Partner’s point of entry to the Network.
- The hardware and software Partners use to exchange information on the Network.
  - The operational layer between a Partner’s information system and the requesting exchange Partner.
- A Node’s operation is guided by the Exchange Protocol, Functional Specification, and other Network Guidance Documents.
Data or Information Flows over the Network

- Current work is focusing on existing regulatory flows (e.g. NEI, FRS etc.)
- Partners are already expanding beyond these to different kinds of information, from other sources.
Network Benefits

- Allows access to more current information
- Sets the stage for the broader exchange of information to include non-regulatory partners
- Provides for more timely, reliable, standardized and consistent data exchanges between Partners
- Provides an opportunity to reduce current reporting burden
- Enhances potential for data integration
- Gives agencies more control over their own data, and ability to tailor other’s data to their use.
- Trading Partners select and maintain their own web service infrastructure
- Platform independent
Looking Under the Hood: Introduction to Network Operation
The Network Node Supports Four Basic Operations

1. **Administering**: Housekeeping.
2. **Querying**: Querying a partner for some data.
3. **Sending**: Send a set of data to a partner.
4. **Retrieving**: Retrieving from a partner a standard set of data.
Using the Network

- To be “on” the Network you are either a Service Provider or a Service Consumer
  - Most Nodes will be both
  - Some Service Consumers will only use a client

- Exchanges will be:
  - Node-Node (routine, large, secured communications)
  - Consumer-Node (ad-hoc, smaller communications)
Broad Range of Service Provider and Consumer Options

- Network Nodes can be used to:
  - Service Other Nodes: support aggregation of data from other Nodes that can then be displayed on a website.
  - Service Clients: submit retrieval data from a Node using a simple client.
  - Integrate Applications: where a local application (webpage, model or report) retrieves information from one or more Nodes as needed.
  - Provide Node Services: use a “hosted” Node, that interacts with other Nodes as a client, but puts data on the Network.

- Two documents describe/define how this works
Network Exchange Protocol (Protocol)

The *Protocol* is the set of rules that governs the generation and use of valid service requests and responses.
Network Node Functional Specification (Specification)

The *Specification* is a detailed description of a Node’s expected operation that includes:

- A description of the functions the Node will perform
- How those functions are to be invoked
- The output expected from the Node
The Protocol and Specification

- **If you want to build a Node**
  - The Protocol and Specification define the expected operation of all Network Nodes.

- **If you want to send data to a Node**
  - The Protocol defines the expected format of all requests and responses from Nodes.
  - The Network WSDL file could assist you in building a client.
If you want to retrieve data from a Node
   - The Protocol defines the expected format of all requests and responses from Nodes.
   - The Network WSDL file could assist you in building a client.

But many users will not need to interact with these directly—they will not care, they just want their data.
Expectations for the v1.0 Protocol and Specification

- The Protocol and Specification have an expected shelf life of between 12 and 24 months.
- The documents are forward-looking.
- The Protocol and Specification generically describe Network operations.
- Future work and experience will define very specific flow business processes.
Basic Network Technologies and Standards
### Defining Network Standards and Stack

<table>
<thead>
<tr>
<th>Discovery Description</th>
<th>UDDI, WSDL</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML Messaging</td>
<td>SOAP, XML</td>
</tr>
<tr>
<td>Transport</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Security</td>
<td>SSL</td>
</tr>
</tbody>
</table>

#### Key Components
- **Universal Description, Discovery and Integration**
- **Web Services Description Language**
- **eXtensible Markup Language**
- **Simple Object Access Protocol**
- **HyperText Transfer Protocol**
- **Secure Sockets Layer**
The WSDL file is a machine readable description which provides a central place where the parties to a trading partner agreement can store new service descriptions for subsequent retrieval.

For a given web service, its WSDL file describes four key pieces of data:
- Interface – information describing all available functions/methods.
- Data type – information for all message requests and message responses.
- Binding – information about the transport protocol to be used.
- Address – information for locating the specified service.
How the Network Uses WSDL

- WSDL represents the contract between the service requester and the service provider.
- Using WSDL, a consumer can locate a web service and invoke any of its available functions.
- WSDL aware tools enable the consumer to automate this process.
Discovery

UDDI*

- This layer is responsible for centralizing services into a common registry and providing publishing/finding functionality.
- The Exchange Network will create and operate one private UDDI registry shared by all Network Nodes.

* Currently under development by EPA/CDX
Using the Node:
The Building Blocks for Information Exchange
# Methods for Network (Hence Node) Operations

<table>
<thead>
<tr>
<th>Interface</th>
<th>Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>NodePing, GetServices</td>
</tr>
<tr>
<td>Security</td>
<td>Authenticate, Authorize*</td>
</tr>
<tr>
<td>Querying</td>
<td>Query, Execute</td>
</tr>
<tr>
<td>Sending</td>
<td>Submit, GetStatus</td>
</tr>
<tr>
<td>Retrieving</td>
<td>Notify, Download, Solicit</td>
</tr>
</tbody>
</table>

* Currently under development by EPA/CDX
Putting it all Together in a Transaction: Query

Requester

Authenticate (userId, credential, authMethod)

securityToken

GetServices (securityToken, ServiceType)

GetServicesResponse

list of available queries

Query (securityToken, source, request, rowId, maxRows)

QueryResponse(ResultSet)
<table>
<thead>
<tr>
<th>Business Need</th>
<th>Current Approach</th>
<th>Network Options</th>
<th>Node Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodic/ Occasional Information sharing with a Peer</td>
<td>E-mail Attachments, FTP, Website posting</td>
<td>NA, unless volume or frequency increases (see below)</td>
<td>NA</td>
</tr>
<tr>
<td>Routine Information Sharing with a Peer (especially secured or confirmed)</td>
<td>Batch uploads, email, FTP</td>
<td>Node to Node, or use of a hosted node.</td>
<td>Solicit/Download/Query (Pull)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Submit (Push)</td>
</tr>
<tr>
<td>Automatic request for ad-hoc information</td>
<td>Custom software</td>
<td>Node to Node, or client to Node</td>
<td>Query (Pull)</td>
</tr>
<tr>
<td>Automated collection of data from multiple peers</td>
<td>Multiple Telephone Calls</td>
<td>Node to Node interactions</td>
<td>Solicit/Query (Pull)</td>
</tr>
</tbody>
</table>
Building the Vehicle:
A Partner Node
Components of Node Building

Supporting Documents

- Network WSDL
  - March 14 2003

- Protocol
  - March 14 2003

- Specification
  - March 14 2003

- Implementation Guide
  - April 2003

- Demonstrated Node Configuration (DNC)
  - May 2003

- Security Guidelines
  - May 2003
## Node 1.0: Diverse Database Environments, Hardware, and Middleware

<table>
<thead>
<tr>
<th>State</th>
<th>Database Environment</th>
<th>Hardware</th>
<th>Middleware</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE</td>
<td>SQL Server 2000</td>
<td>Dell PowerEdge Dual Pentium</td>
<td>.NET 1.0</td>
</tr>
<tr>
<td>ME</td>
<td>Oracle 9.2</td>
<td>Sun E6500</td>
<td>Oracle 9iAS</td>
</tr>
<tr>
<td>MS</td>
<td>Oracle 8i</td>
<td>Dell PowerEdge 2650</td>
<td>.NET 1.0</td>
</tr>
<tr>
<td>NH</td>
<td>Oracle 8.0</td>
<td>Compaq Proliant ML370</td>
<td>BizTalk Server 2000</td>
</tr>
<tr>
<td>NM</td>
<td>TEMPO</td>
<td>Sun SunFire 280R</td>
<td>WebSphere v4.05</td>
</tr>
<tr>
<td>NE</td>
<td>DB/2</td>
<td>Gateway 2000 server</td>
<td>XAware XA-Suite</td>
</tr>
<tr>
<td>UT</td>
<td>Oracle 9i</td>
<td>Compaq Proliant server</td>
<td>Sybase EASserver</td>
</tr>
<tr>
<td>CDX</td>
<td>Oracle 9i</td>
<td>Dell PowerEdge Dual Pentium</td>
<td>BEA WebLogic</td>
</tr>
</tbody>
</table>
Network Security
Four Basic Network Security Needs

- Authentication
- Authorization
- Confidentiality
- Message Integrity
Current Network Security

- Protocol and Specification development focused on creating a basic, extensible, and flexible security model.
  - The current protocol and specification places the burden of security on Network Partners.
  - EPA CDX will drive the security in the first generation of the Network.
    - Most initial flows will be Partner to CDX.
    - CDX will provide authentication and authorization for all Network Partners through the Network Authentication and Authorization Services (NAAS).
Security
Network Authentication and Authorization Services (NAAS)

- Network Authentication and Authorization Services (NAAS) are centralized security services.
- Security tokens and assertions issued by NAAS are trusted and accepted by all Network Nodes.
- NAAS provides a set of standard web services across the network, accessed by network users and services providers.
- Operations defined in NAAS must be conducted over a secure SSL channel using 128 bit encryption.
- CROMERR Security
Proposed NAAS Structure

- Network Authentication Service
- Network Authorization Service
- Network Identity Management Service

Integrated Security Managements
- User Management
- Policy Management
- Intrusion Management
- Vulnerability Management

User Identity Store
Security Policy Store
Intrusion Detection Rules

NAAS Web Service Interface

Request → Response
# NAAS: Advantages and Disadvantages

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplified Implementation</td>
<td>Increased Overhead</td>
</tr>
<tr>
<td>Enhanced Security</td>
<td>NAAS Dependency</td>
</tr>
<tr>
<td>Cost Effective</td>
<td></td>
</tr>
<tr>
<td>Highly Extensible</td>
<td></td>
</tr>
<tr>
<td>Supports Single Sign-On (SSO)</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td></td>
</tr>
</tbody>
</table>
Next Steps
## Node 1.0 Products

<table>
<thead>
<tr>
<th>Product</th>
<th>Status</th>
<th>Date of Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Protocol</td>
<td>✓</td>
<td>March 14, 2003</td>
</tr>
<tr>
<td>Functional Specification</td>
<td>✓</td>
<td>March 14, 2003</td>
</tr>
<tr>
<td>Network WSDL</td>
<td>✓</td>
<td>March 14, 2003</td>
</tr>
<tr>
<td>Implementation guide</td>
<td></td>
<td>April 2003</td>
</tr>
<tr>
<td>Demonstrated Node Configurations</td>
<td></td>
<td>May 2003</td>
</tr>
<tr>
<td>Security Guidelines</td>
<td></td>
<td>May 2003</td>
</tr>
</tbody>
</table>
Lessons Learned

- Immaturity in Web Services Standards and Network Tools:
  - UDDI defined in Protocol and Specification but no Network UDDI infrastructure exists
  - Limitations in message encoding
  - DI ME implementations differ by platform
  - Limited functionality of WSDL Tools

- Mapping the ‘back-end’ systems to the Schema is one of the most challenging and time intensive tasks.

- Difficult to provide accurate cost estimates – too many variables.

- Node builders should be able to use Node code from similar Nodes. The Node 1.0 team is creating Demonstrated Node Configurations.
**Recommendations to the NSB**

The Node 1.0 Group Recommends Support for the Following Activities:


The Node 1.0 Group has proposed the creation of a Network Operations Group (NOG) that will oversee the staffing and organization of these activities.
Node Building Resources
The Network Exchange Website
http://www.exchangenetwork.net

- Supporting Documents
- Node Updates
- Frequently Asked Questions*
- Discussions Groups*
- Implementer Tool Box*

* Currently under development
Questions/Discussion