

**iWay's Intelligent Adapter for EDIINT provides AS1, AS2, and AS3 connectivity to eliminate VAN costs through standard Internet technologies like e-mail, HTTP, and FTP.**

### Product Highlights

- **Delivers transaction integrity, security, and non-repudiation** over the Internet without using a Value-Added Network (VAN)
- **Manages all HTTP (AS2), SMTP (AS1), and FTP (AS3) connections**
- **Computes and delivers or validates** the appropriate public-key Message Integrity Checks to ensure message validity
- **Provides and handles Message Disposition Notifications (MDNs)** as receipts within an EDI transaction
- **Specifies and handles the appropriate MIME and S/MIME content types** for each message



**EDIINT**

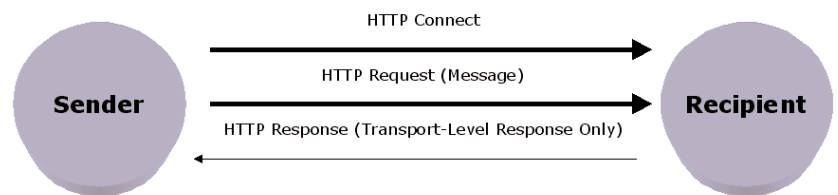
## iWay Intelligent Adapters for EDIINT Accelerating TCO Reduction Through Internet-Based EDI

### Security, Reliability, and Non-Repudiation Without a VAN

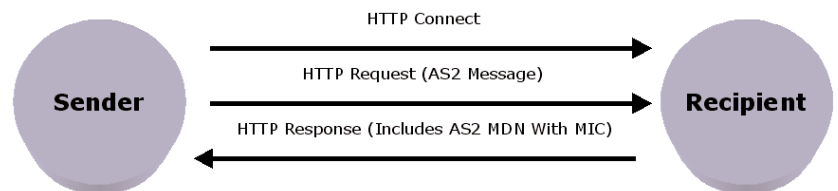
Electronic Data Interchange (EDI) technologies were among the earliest used to promote business-to-business information exchange. Messages of a specific format were emitted to Value-Added Networks, or VANs, which would be responsible for ensuring that they were securely transmitted to the recipient once and only once. The VAN was also responsible for non-repudiation – ensuring that the sender couldn't claim that someone else had sent the message.

While this system has worked reliably for decades and continues to be used by large companies today, it has its drawbacks. Chief among them is the high cost of the VAN, which may charge users setup fees, per-transaction fees, and correction fees when an incorrectly formatted message is sent.

The Internet Engineering Task Force (IETF) created the Electronic Data Interchange-Internet Integration (EDIINT) working group to promote the use of the Internet for secure, reliable, and non-repudiable transactions.



**Before: Synchronous HTTP response provides only transport-level verification that message was received.**



**After: AS2 HTTP response may provide a signed Message Disposition Notification with a Message Integrity Check to ensure the message was not corrupted in transit, increasing reliability and security.**

The EDIINT working group developed Applicability Statements 1, 2, and 3 (AS1, AS2, and AS3) to use SMTP e-mail, HTTP, and FTP respectively, to achieve this goal. Both AS1, AS2, and AS3 use encryption and digital signatures to ensure secure transmissions, and appropriate handshaking to ensure reliability and non-repudiation.

Organizations that move to AS1, AS2, and AS3 can achieve dramatic Total Cost of Ownership (TCO) reductions over traditional VANs.

### **Easy-to-Use EDIINT**

iWay's AS1, AS2, and AS3 adapters provide a simple mechanism for supporting all aspects of EDIINT-based document interchange.

When an iWay adapter transmits a document using EDIINT, it follows this process:

- The requesting application packages an XML document that contains all of the relevant information.
- If desired, the requesting application sends the document to an iWay EDI adapter by putting it in a message queue, dropping it in a directory, or invoking an FTP or HTTP command. iWay has also developed plug-ins for some of our partner tools, making the handoff to the EDI adapter transparent to the user.
- The iWay EDI adapter handles the validation of the document and its transformation into an appropriate EDI format. Some iWay EDI adapters are industry-specific, such as SWIFT, HIPAA, and UCCnet, while others conform to broader standards such as ASC X12 and EDIFACT. Other payloads, such as XML, are also supported.
- The iWay EDI adapter sends the message to the iWay AS1, AS2, or AS3 adapter.
- The iWay AS1, AS2, or AS3 adapter wraps it with the appropriate headers, signs and/or encrypts as appropriate, and delivers it over the Internet.
- The receiving party may use a synchronous or asynchronous Message Disposition Notification (MDN), or receipt, to convey the delivery status of the message.
  - If the receipt is asynchronous, the receiving party returns a transfer-layer acknowledgment of a successful transmission, and later returns an MDN through the appropriate mechanism (typically HTTP).
  - If the receipt is synchronous, the receiving party immediately responds with an MDN.
- The MDN may contain the results of a one-way mathematical hash of the original message. This value, called the Message Identification Code (MIC) or “message digest,” can be used by the iWay adapter to verify that the content that was received is the same as the content that was sent.
- The MDN or appropriate error codes can be returned via a variety of transports to the requesting application.

The iWay AS1, AS2, and AS3 adapters also receive EDIINT messages in a similar way. They decrypt, authenticate, return status using MDNs with MICs as appropriate, optionally transform into XML using the appropriate EDI adapter, and hand off the received, validated, and transformed message to the appropriate application, middleware, or tool.

## Features and Benefits of the iWay EDIINT Adapters

**Ease of EDI document handling.** Because the EDIINT adapters work in conjunction with any other iWay EDI adapters, users can take advantage of iWay's sophisticated XML-to-EDI transformation capabilities. Users can work with their own tools, familiar formats, and easy-to-debug documents before handing the message off to iWay adapters to handle the complex validation, transformation, encryption, and handshaking required by the EDIINT specifications.

**Ease of providing security, reliability, and non-repudiation.** iWay's EDIINT adapters use Public Key Infrastructure (PKI) technology to manage security, reliability, and non-repudiation. They create X.509 certificates that can be stored and exported from a keystore along with third-party certificates. Messages and MDNs can be triple-DES encrypted and/or signed using private or public keys for maximum flexibility in targeting and validating recipients, and to ensure that the sender cannot repudiate a message. MDNs and MICs provide assurance that the message was not tampered with en route.

All of these features are available transparently to end users, allowing them to focus on putting the right data in the payload instead of the intricacies of encryption, digital signatures, validation, non-repudiation, and receipt handling.

**Data integrity assurance.** Message Identification Codes (MIC), or "message digests," are hash values computed using the standard SHA1 or optional MD5 algorithm based on the content of the EDIINT message and the recipient's private key. The MIC can be sent to the sender in the MDN, or receipt, so that the sender can verify that the received message was the same as the sent message.

**Certified EDIINT compliance.** iWay Software's EDIINT technologies have been fully certified by the Drummond Group, earning the eBusinessReady logo after rigorous interoperability testing. For more information about certifications, visit [www.ebusinessready.org](http://www.ebusinessready.org).

## Find Out More

To learn how iWay's EDIINT adapters can work in conjunction with other iWay integration solutions, messaging middleware, third-party application servers and integration brokers, and business-to-business solutions, please visit one of our branch offices, contact iWay Software at [info@iwaysoftware.com](mailto:info@iwaysoftware.com), or call toll-free **(866) 297-4929**.

