Systrends

NAESB EDM Overview

Dick Brooks

VP Secure Systems

Dick.Brooks@systrends.com

Systrends

Agenda

- Brief History of EDM
- Functional Overview
- EDM's influence on EDIINT AS2 and ebXML/web services
- Brief Review of GISB EDI/EDM 1.4
- Version 1.5 enhancements (June 30, 2001)
- Version 1.6 enhancements (June/July, 2002)

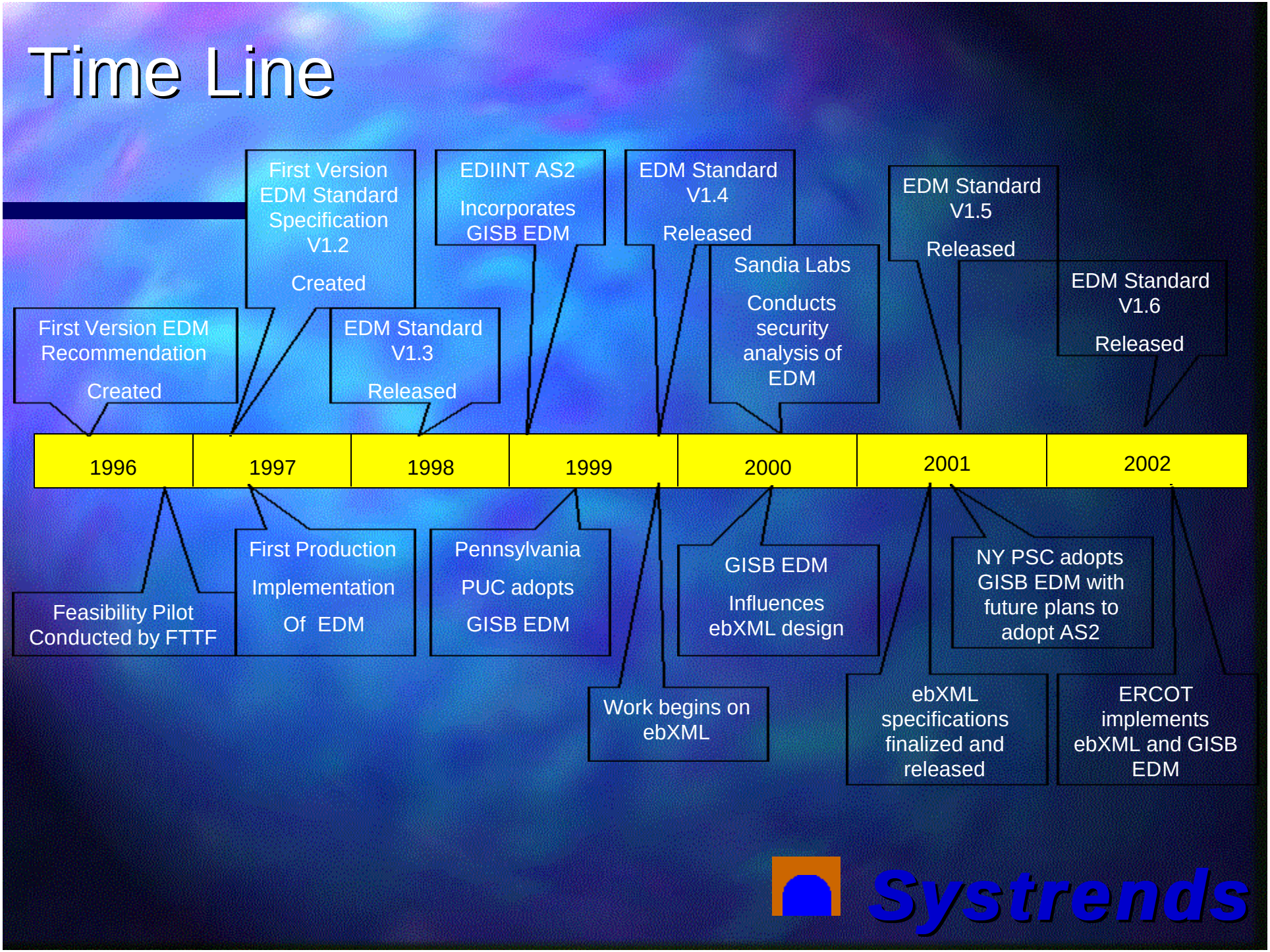
Systrends

EDM Overview

- Initial Goals and Objectives
  - Create a reliable transport protocol for the exchange of EDI documents
  - Utilize Internet technologies to minimize cost
  - Ensure a high degree of security
    - Privacy – addressed with PGP encryption
    - Integrity/Authentication – addressed with PGP digital signatures
    - Access control using username/password
  - Support both batch and interactive file uploads

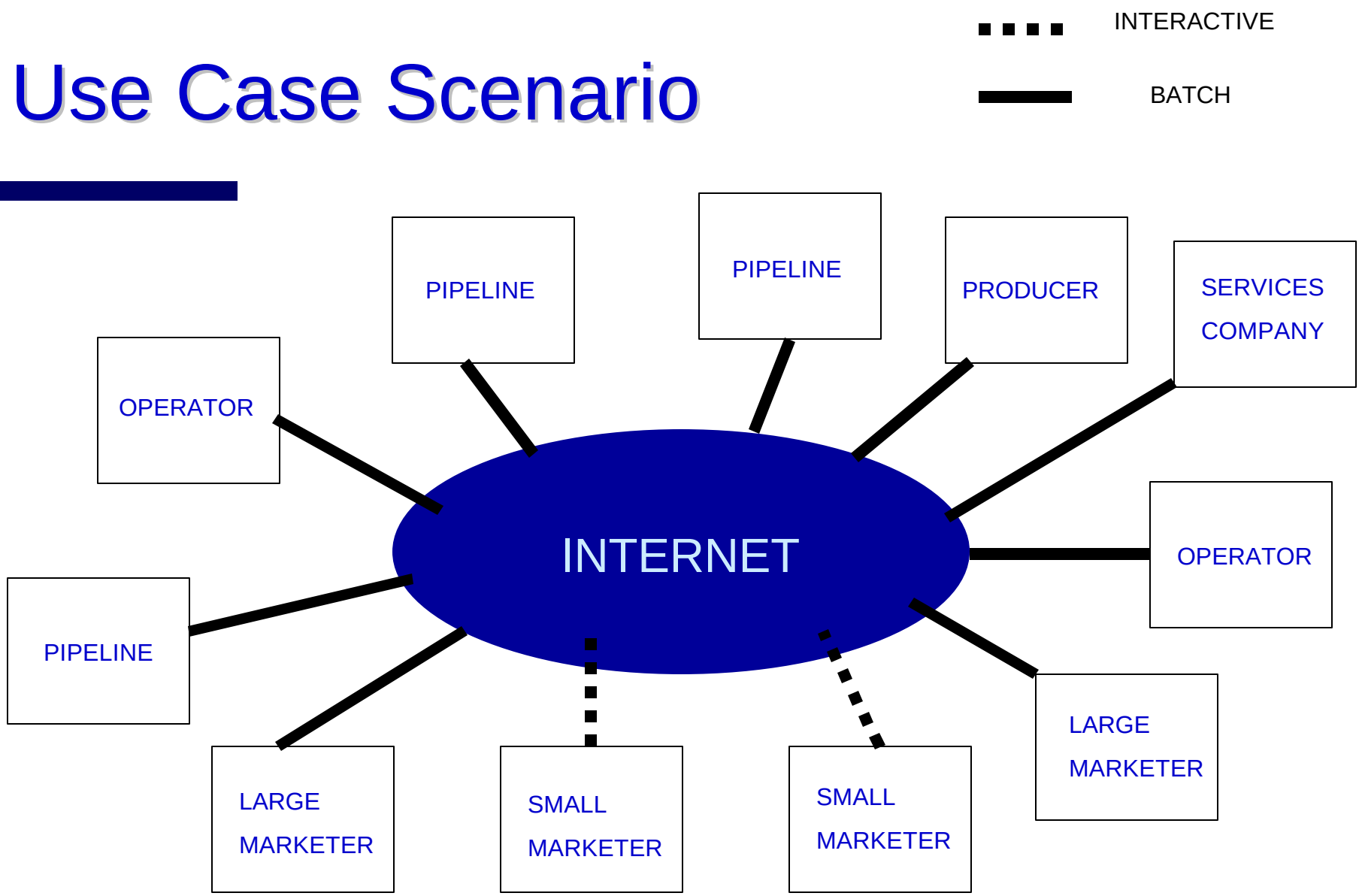
Systrends

Time Line



Systrends

Use Case Scenario



Systrends

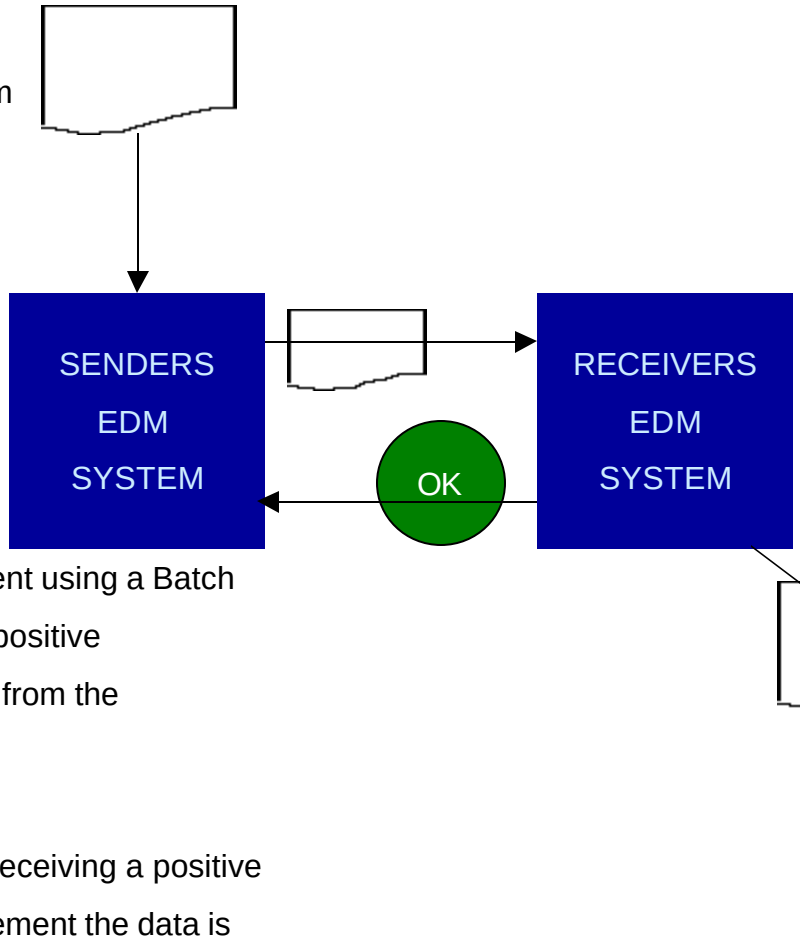
EDI/EDM File Exchange Overview

1. An EDI transaction Is created by a backend system And is forwarded to the EDM System for processing

2. The Senders EDM System encrypts/signs the EDI Data using PGP

3. The encrypted data is sent using a Batch Browser, which waits for a positive Delivery acknowledgement from the receiver

4. After receiving a positive Acknowledgement the data is Considered delivered and is typically archived by the sender



5. After sending a positive Delivery acknowledgement the Receivers EDM system uses PGP To decrypt/verify the data received. This exposes the original EDI data.

6. The EDI data is passed to a Backend application (translator) For further processing.

Systrends

Batch Mode Functionality

- Data is sent directly to a trading partner's "designated site URL"
- A "Batch Browser" is used to send data
- Batch Browsers can be "event driven" or run at regularly scheduled intervals
- A Web/CGI server must be available online to receive incoming data
- Recommendations are defined for failure/retry

Systrends

Interactive Mode Functionality

- Allows user to send data using a standard web browser
- Positive delivery acknowledgement is displayed in users browser
- There is no ability for an interactive user to “receive” using the EDM standard
- INTERACTIVE UPLOAD DEMONSTRATION

Systrends

EDM's Influence on AS2 and ebXML

- ALL of GISB EDM 1.5 functionality is contained in EDIINT AS2
- AS2 contains two profiles:
  - E-mail over HTTP (AS1 over HTTP)
  - HTTP standard file upload (GISB EDM - RFC2388)
- ebXML assimilates GISB EDM functionality, but uses XML to represent data elements
- ebXML adds support for push-pull

Systrends

GISB EDI/EDM Version 1.4 Overview

- EDI/EDM Technologies/Standards
  - HTTP 1.0
  - PGP version 2.6 compatible crypto
  - Multipart/form-data spec RFC1867
- Outbound Header Data Element Names
  - TO – DUNS Number of the recipient
  - FROM – DUNS Number of the sender
  - INPUT-FORMAT – type of data sent (e.g. X12)
  - INPUT-DATA – encrypted business data
  - TRANSACTION-SET (optional) – name of transaction sent in INPUT-DATA (e.g. 850NMST)

Systrends

GISB EDI/EDM Version 1.4 Overview

- Receipt Data Elements
  - TIME-C - Date/Time transfer completed
  - REQUEST-STATUS – error or success message
  - SERVER-ID – Name of server issuing receipt
  - TRANS-ID – Token used for tracking purposes

Systrends

Open Issues with version 1.4

- Sandia Labs List of Security Issues
  - Some Transactions Not Digitally Signed
    - **Error Notifications**
    - **Timestamps**
  - Some Data Not Kept Confidential
    - **Error Notifications**
    - **Timestamps**
    - **Username/Passwords**
  - Message Replay Allowed
- Cost of PGP is rising

Systrends

GISB EDI/EDM Version 1.5

- Technologies Used
  - HTTP 1.0
  - PGP 2.6 compatible crypto
  - Multipart/form-data spec RFC1867
  - EDIINT AS2 compliant
  - PGP/MIME RFC2015
  - EDI MIME types per RFC1767
- Addresses the following Sandia issue with 1.4:
  - Some Transactions (receipts,error notifications) not digitally signed

Systrends

Features of version 1.5

- Support for signed receipts and error notifications
- Version identifier
- EDI payloads identified with standard MIME types per RFC 1767
- EDIINT AS2 compliant, more header data elements

Systrends

Open Issues with version 1.5

- Sandia Labs List of Security Issues
  - Some Data Not Kept Confidential
    - Error Notifications
    - Timestamps
    - Username/Passwords
  - Message Replay Allowed
- Cost of PGP is rising to “high levels” and uncertainty over PGP’s future

Systrends

NAESB EDI/EDM version 1.6

- Technologies Used
  - HTTP 1.1
  - Secure Sockets Layer V3
  - PGP 2.6 or OpenPGP compatible crypto
  - Multipart/form-data spec RFC1867
  - EDIINT AS2 compliant
  - PGP/MIME RFC2015
  - EDI MIME types per RFC1767

Systrends

Issues Addressed in 1.6

- Addresses the following open issues with 1.5
  - Sandia Labs List of Security Issues
    - Some Data Not Kept Confidential
      - **Error Notifications**
      - **Timestamps**
      - **Username/Passwords**
  - Message Replay Allowed
  - Cost of PGP is rising to “high levels” and uncertainty over PGP’s future

Systrends

Features of version 1.6

- Requires use of 128 bit SSL to protect usernames, passwords, error notifications and timestamps (receipts)
- Includes a unique Reference Number on outbound messages for tracking/auditing purposes and to prevent replay attacks
- Allows use of “free” version of PGP (OpenPGP)

Systrends

Open Issues with Version 1.6

- No “formal” support for XML **
- No support for push-pull operations (e.g. mailboxing for smaller trading partners on a larger trading partners server) (not essential in some environments)

**NAESB Executive Committee authorized use of a temporary workaround

Systrends

Questions

Systrends