



PsypherTMEDI

A Security Envelope for Any Transaction File

When the same security product can be used by both the sender and the receiver, PsypherEDI may be all you need to protect all types of sensitive business transaction files. PsypherEDI consists of two main components: an interactive menu-driven utility to manage a trading partner database of encrypted keys and security options, and a batch component to automatically secure transaction files on a regularly scheduled basis. For files being transferred from one location to another, PsypherEDI provides any combination of four separate options:

Data Encryption

PsypherEDI provides confidentiality using a variety of strong encryption algorithms (56-bit DES, 112-bit Triple DES, 160-bit Blowfish, and 256-bit AES). PsypherEDI can access computer hardware features such as IBM's Integrated Cryptographic Service Facility (ICSF) on mainframes for improved performance and maximum security for key management.

Message Authentication

PsypherEDI verifies the origin of the transmitted file and its integrity using X9.9 Message Authentication Codes (MACs) or RSA digital signatures.

Data Compression

PsypherEDI saves transmission time and money by compressing data using the popular X9.32 compression algorithm (also known as LZW compression).

Text/Data Control

When necessary, PsypherEDI simplifies communication through multiple Value Added Networks (VANs) using text-filtering techniques to avoid sending binary data.

Secure Any File With PsypherEDI

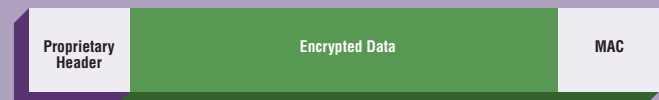
X12 and EDIFACT

Embedded security includes encrypted segments of data groups and transaction sets within a transaction file. This file has a clear header and footer for routing.



PsypherEDI

"Security envelope" – the entire message is hidden. A proprietary header contains no routing information. A MAC at the end of the secured file is used to verify the origin and integrity of the data.



Application vs. Transport Level Security

Application level security is a better solution because it protects data at every stage, instead of only during the communications link.

Before Processing	Awaiting Transport	Comm Link	Awaiting Processing	After Processing
Clear Data	Encrypted Data	Encrypted Data	Encrypted Data	Clear Data
Clear Data	Clear Data	Encrypted Data	Clear Data	Clear Data



Tools Designed for the Real World

Key Management and all other processing occurs on the same platform in order to simplify control of your computing environment. Robust password protection of administrative functions, role-based user definitions, and key entry by components increase flexibility without compromising security.

The software includes many ease-of-use features such as the export/import of trading partner definitions, a complete audit log, optional trace facility, key check values, and built-in test keys.

Psypher Security Suite

PsypherEDI is part of the Psypher Security Suite, which also contains advanced support for other data security needs:

PsypherTMX12

Supports the internal X12.58 security structures that protect X12-formatted business transaction files.

PsypherTMEDIFACT

Supports the internal ISO 9735 security structures that protect EDIFACT-formatted business transaction files.

PsypherTMOPS

Supports file transfers using the OpenPGP formats defined in RFC1991 and RFC2440.

General Security Options

General security options can be set for each trading partner.

```
----- PsypherEDI - Edit PSYPHER Securing Options -----
Command ==>
Company/Dept Name: Big Bank      Options Set Name.: BANKOPTS

SECURING.....: Service (A-Authenticate, E-Encrypt, B-Both, N-None) ==> B
OPTIONS
Filter (H-Hex, A-Ascii, N-None) ==> N
Algorithm (D-DES, T-Triple Des, B-Blowfish, 4-40 Bit) ==> T
Compression (Y, N) ==> Y
UNSECURING...: Short Records Pad (char, hex) ==> P
OPTIONS
Long Records (W-Wrap, F-Fold, T-Truncate) ==> W
Trim Trailing Blanks (Y, N) ==> Y
Automatic Character Set Translation (Y, N) ==> Y
Commands.....: ( ADD (F5)   - Add a Field Definition )
                ( ENTER   - Save Changes )
                ( END     - Cancel Changes and Return )
Select Codes.: ( E -Edit, D -Delete)

FIELDS:  Col      Len      Type      Service
***** Bottom of data *****
```

Cross Platform Support

Like all Prime Factors products, PsypherEDI provides for backward compatibility with previous versions of the product and is available for mainframes, AS/400s, HP9000s, Suns, RS/6000s, and PCs running Windows or Linux. To arrange a 30-day trial at no charge, visit our web site at www.primefactors.com.

Field Level Security

Special security options are available for individual data fields.

```
----- PsypherEDI - Set PSYPHER Field Definition -----
Command ==>

Company/Dept Name: Big Bank      Options Set Name.: BANKOPTS

Special Processing for Specific Fields. Define the field location
and processing required:

Starting Column in Each Record ==> 1
Length of the Field ==> 0
Optional New Length (0-don't change length) ==> 0
Pad when new length is longer (char, hex) ==>
Type of Field (C-Character, I-Integer, B-Binary) ==> C
Encrypt the Field (Y, N) ==> Y

Press ENTER to Set Field Definition.
Enter END Command to Cancel and Return to Previous Menu.
```

Audit Log

The audit log shows all security-related activity, not just the errors.

```
----- PsypherEDI - Audit Log ----- Row 190 of 207
Command ==>

Press ENTER to Return or Enter COPY (F11) Command to Copy Display to a File.

2002/06/11 06:55:42 ERR154 (MARY) No interchanges processed, all interchanges
2002/06/11 06:55:42 INF148 were copied to the reject file.
2002/06/11 06:55:42 INF148 (MARY) RECVX12 function failed: 03
2002/06/14 00:04:28 INF423 (MARY) Partner ID changed: From ID: TIPSY SecId:
2002/06/14 00:04:28 TIPSYP, To ID: ACHPSYCO SecId: ACHPSYCO, Records
2002/06/14 00:04:28 Changed: 2
2002/06/14 00:04:28 INF409 (MARY) Party Relationship Added/Changed for:
2002/06/14 00:04:30 INF409 ACHPSYCO
2002/06/14 00:22:15 INF409 (MARY) Party Relationship Added/Changed for:
2002/06/14 00:22:15 ACHPSYCO
2002/06/14 01:08:09 INF401 (MARY) Data secured OK. Partner: ACHPSYCO,
2002/06/14 01:08:09 Transaction: Date: 06/14/2002, Time: 01:08:08,
2002/06/14 01:08:09 Records: 8, Triple DES
2002/06/14 01:08:09 INF425 (MARY) Compression: 33%
2002/06/14 01:13:32 ERRO45 (MARY) Invalid trading partner ID. Must be four or
2002/06/14 01:13:32 more characters long.
2002/06/14 01:13:32 INF148 (MARY) Psypher Secure function failed: 01
2002/06/14 01:13:33 INF148 (MARY) SENDPSY function failed: 01
```

Download
PsypherTMEDI
for a **30 day**
free
trial.



PRIME FACTORS, INC.
your key to data security