

# PRIME FACTORS, INC.

your key to data security



## Psypher™X12

### Dependable Security for X12 Transaction Files

When there is a requirement to protect 820 payments or any other X12 business transaction, PsypherX12 can complement any X12 translator by adding necessary security functions. Consisting of two main components, PsypherX12 has an interactive menu-driven utility that manages a trading partner database of encrypted keys and security options, and a batch component that automatically secures transaction files on a regularly scheduled basis. PsypherX12 conforms to the X12.58 standard specifications and provides the following important features:

#### Data Encryption

Confidentiality is ensured using strong encryption algorithms (56-bit DES, 112-bit Triple DES, and 168-bit Triple DES).

#### Message Authentication

PsypherX12 verifies the origins of transmitted files and their integrity using either the X9.9 Message Authentication Codes (MACs) developed by the financial industry or RSA digital signatures with X.509v3 certificates.

#### Data Compression

PsypherX12 reduces transmission time and expense by compressing data using the popular X9.32 compression algorithm (also known as LZW compression).

#### Text/Data Control

Communication through multiple Value Added Networks (VANs) can be simplified using text-filtering techniques to avoid sending binary data.

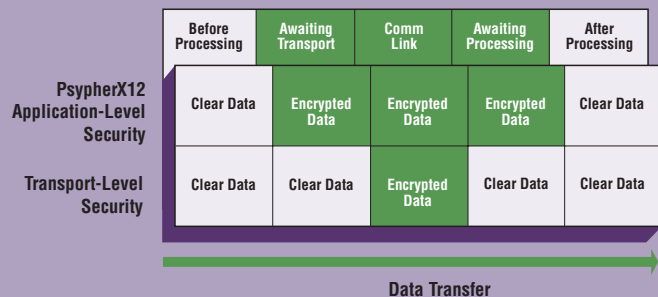
#### Ensure Data Security with PsypherX12

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.



#### 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.



## 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.

PsypherX12 also provides interoperability with other vendors' X12 security products which support the X12.58 v3050 or v4010 security standard.

## Cross Platform Support

Like all Prime Factors products, PsypherX12 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](http://www.primefactors.com).

## The Psypher Security Suite

PsypherX12 is part of the Psypher Security Suite, which also contains advanced support for other data security needs:

### Psypher<sup>™</sup>EDIFACT

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

### Psypher<sup>™</sup>EDI

Provides a proprietary security envelope for transaction files of any format, including X12 and EDIFACT.

### Psypher<sup>™</sup>OPS

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.

```
----- PsypherX12 Security Options ----- Row 1 of 2
Command ==>

Company/Dept Name: Big Bank
Partner Name ....: Local Credit Union

Partner is Active? =====> Y ( Y -Yes, N -No)
Level for Security =====> G ( G -Group, T -Trans)
Comment =====>

Specify Securing Options in the Following Group Security Specifications:
Selection Codes: E - Edit Group
                  D - Delete Group
Commands : ADD (F5) - Add a Group          ENTER - Save Changes
            COMM (F6) - Communication Options END - Cancel Changes
            ISA (F10) - ISA Options
            ENC (F11) - Encryption/Filtering Options

Sel  ID      Service      Method      Mode      Filter
    ALL  AUT ENC      DES        CBC        None
    FA    None

***** Bottom of data *****
```

## ISA Options

ISA options can be set for each trading partner.

```
----- PsypherX12 - ISA Options -----
Command ==>

Company/Dept ID to Use .....: BIGBANK
Company/Dept Security ID to Use .....
ID ..: BIGBANKSECID
Partner Name .....: Local Credit Union
X12 Standards Version (0=3030, 1=4010) =====> 1
Use Machine native CBC zero padding =====> Y (Y, N)
Use 16 byte Hex encryption IV (Initialization Vector) ==> Y (Y, N)
Generate Functional Acknowledgment Messages (997s) =====> N (Y, N)
Use Fixed Delimiters (*, LF) for authentication =====> N (Y, N, A)
Leave Digital Signature segments in received transaction=> N (Y, N)
Public Key Certificates require special extension info => Y (Y, N)
Partner is in Production Status =====> N (Y, N)
ISA Message Separators
Terminator ==> 1C Element ==> 1D Sub Element ==> 1F
ISA Header Information
ID Qualifier =====> ZZ Test Indicator ==> P (P, T)
Control Number ==> 000000001

Enter USE (F10) Command to Set Company IDs to Use With This Partner.
Press ENTER to Save Changes and Return to Previous Display.
Enter END Command to Cancel Above Field Changes, Return to Previous Display.
```

## Audit Log

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

```
----- PsypherX12 - Audit Log ----- Row 174 of 191
Command ==>

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

2002/06/11 06:36:42 CREDITUNION
2002/06/11 06:41:06 INF419 (MARY) ID: RA, Secured, ISA Ctrl# 211290000,
2002/06/11 06:41:06 Receiver: CREDITUNION, GRP Ctrl# 211290000, Auth:
2002/06/11 06:41:06 KMAD01(089531), Enc: KDED01(36F09F)
2002/06/11 06:41:06 INF401 (MARY) data secured OK. Partner: CREDITUNION,
2002/06/11 06:41:06 Transaction: Date: 11/29/1997, Time: 19:08, ISA
2002/06/11 06:41:06 Ctrl# 211290000
2002/06/11 06:55:38 ERR156 (MARY) Interchange message is not to us. ID:
2002/06/11 06:55:38 BIGBANK
2002/06/11 06:55:39 ERR152 (MARY) Transaction in Error: Date: 04/15/2002,
2002/06/11 06:55:39 Time: 08:42, ISA Ctrl# 000000006
2002/06/11 06:55:40 ERR156 (MARY) Interchange message is not to us. ID:
2002/06/11 06:55:40 BIGBANK
2002/06/11 06:55:40 ERR152 (MARY) Transaction in Error: Date: 04/15/2002,
2002/06/11 06:55:40 Time: 08:42, ISA Ctrl# 000000007
2002/06/11 06:55:42 ERR154 (MARY) No interchanges processed, all interchanges
2002/06/11 06:55:42 were copied to the reject file.
2002/06/11 06:55:42 INF148 (MARY) RECVX12 function failed: 03
```

Download  
**Psypher<sup>™</sup>X12**  
for a **30 day**  
**free**  
**trial.**



**PRIME FACTORS, INC.**  
your key to data security