

Authora's EDGE (Encrypted Data Gateway Engine) is compliant with the OpenPGP standard, OpenPGP is the most widely used standard for securing emails and secure file transfer. EDGE follows IETF RFC 1991 and IETF RFC 2440. In addition, EDGE uses the same syntax as other OpenPGP command-line product for an easy integration or replacement to an existing solution. A message encrypted with another OpenPGP client can be handled by EDGE. It is also possible to generate encrypted/signed message for older Open PGP clients like PGP 2.6.x or ViaCrypt PGP.

- | | |
|---|--|
| <ul style="list-style-type: none"> ↓ Version 2/3 key handling ↓ Version 4 key handling ↓ RSA key handling ↓ DSS/DH key handling ↓ Generation of files compatible with PGP2.6.2 ↓ Public-key encryption ↓ Secret-key encryption ↓ Secret-key encryption and digital signature ↓ Session key display ↓ Session key file support ↓ Compression level tuning | <ul style="list-style-type: none"> ↓ Automatic disabling of text mode ↓ Progression information during encryption ↓ Log File ↓ Filter mode ↓ Multiple password support ↓ Configurable password retry ↓ Import of X.509 certificates ↓ Use of SmartCard to digitally sign and decrypt data ↓ FIPS PUB 140 compliant ↓ Power-up tests on request ↓ local X.509 secret keys digitally sign and decrypt data ↓ Configurable import |
|---|--|

FEATURE COMPARISON	EDGE	PGP 6.5.8	PGP 7.0.1	PGP 9.0
Version 2/3 key handling	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Version 4 key handling	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
RSA key handling	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
DSS/DH key handling	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Generation of files compatible with PGP2.6.2	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Public-key encryption	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Secret-key encryption	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Secret-key encryption and digital signature	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Session key display	✓ EDGE	NO PGP 6.5.8	NO PGP 7.0.1	NO PGP 9.0
Session key file support	✓ EDGE	NO PGP 6.5.8	NO PGP 7.0.1	✓ PGP 9.0
Compression level tuning	✓↓ EDGE	NO PGP 6.5.8	NO PGP 7.0.1	NO
Automatic disabling of text mode	✓ EDGE	? PGP 6.5.8	? PGP 7.0.1	✓ PGP 9.0
Progression information during encryption	✓ EDGE	NO PGP 6.5.8	NO PGP 7.0.1	NO

Log file	✓ EDGE	NO	NO PGP 7.0.1	NO
Filter mode	✓ EDGE	✓ PGP 6.5.8	pgp keyserverPGP 7.0.1	✓ PGP 9.0
Configurable import (public keys only, secret keys only, merge only)	✓ EDGE	NO PGP 6.5.8	NO PGP 7.0.1	✓ PGP 9.0
Multiple password support	✓ EDGE	✓ PGP 6.5.8	✓ PGP 7.0.1	✓ PGP 9.0
Configurable password retry	✓ EDGE	Default to 3	Default to 3	NO
Import of X.509 certificates	✓ EDGE Windows only	NO PGP 6.5.8	NO PGP 7.0.1	✓ PGP 9.0
Use of local X.509 secret keys to digitally sign and decrypt messages	✓ EDGE Windows only	NO PGP 6.5.8	NO PGP 7.0.1	NO
Use of SmartCard to digitally sign and decrypt messages	✓ EDGE Windows only	NO PGP 6.5.8	NO PGP 7.0.1	✓ PGP 9.0
FIPS PUB 140 compliant	✓ EDGE Level 4	NO PGP 6.5.8	NO PGP 7.0.1	✓ PGP 9.0
Power-up tests on request	✓ EDGE	NO PGP 7.0.1	NO PGP 7.0.1	✓ PGP 9.0