High-grade Data Security with Ammonit Meteo-40 and AmmonitOR

Measurement data is irreplaceable. To protect your data, Ammonit Meteo-40 data loggers and our online monitoring platform AmmonitOR use the **OpenPGP standard** to encrypt and sign data by utilizing public key cryptography. This standard combines the advantages of asymmetric and symmetric cryptography: secure key transmission and high-speed communication. The implemented public key cryptography consists of public and private keys, which are used to encrypt / decrypt, sign and verify messages.

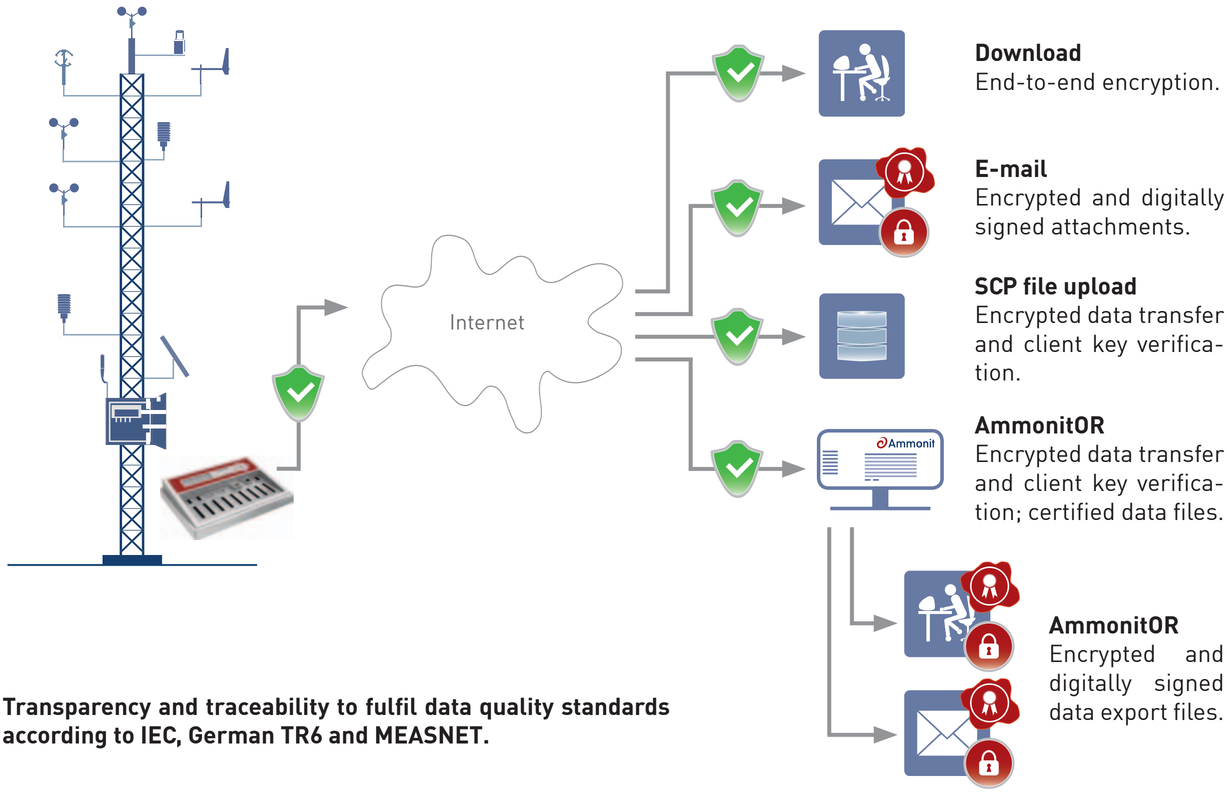
Digital Signature

A digital signature is a mathematical scheme to ensure the authenticity of a digital message or document. A valid digital signature indicates to the recipient that the message was created by a known sender (authentication) and that the message was not manipulated on transit (integrity).

Encryption

Encryption is a process of encoding messages or information in a way that only authorized parties can read it. The message or information is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

Digital signature and encryption with Ammonit Meteo-40 data loggers and AmmonitOR



Download
End-to-end encryption.

E-mail
Encrypted and digitally signed attachments.

SCP file upload
Encrypted data transfer and client key verification.

AmmonitOR
Encrypted data transfer and client key verification; certified data files.

AmmonitOR
Encrypted and digitally signed data export files.

Transparency and traceability to fulfil data quality standards according to IEC, German TR6 and MEASNET.

AFTER ENCRYPTION ONLY THE KEY HOLDER IS ABLE TO DECRYPT FILES SENT BY AMMONIT METEO-40 DATA LOGGERS OR AMMONITOR. IN CASE OF MISSING KEYS, AMMONIT CANNOT DECRYPT CUSTOMER'S FILES AND DATA MAY BE LOST.

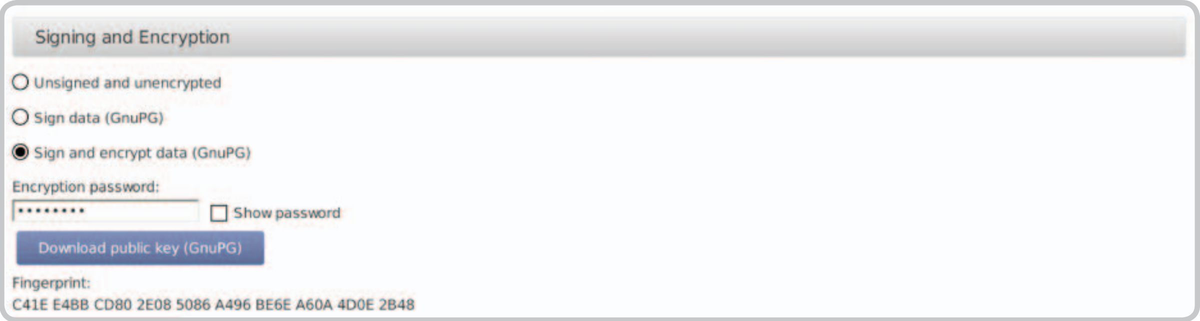
How does data security work on Ammonit Meteo-40 data loggers?

Protecting data sent via email from Ammonit Meteo-40 data loggers

On each Meteo-40, Ammonit installs a unique private key. All files sent via email by Meteo-40 can be encrypted and digitally signed with its individual private key. In order to verify these files, Ammonit provides a public key. To access the original measurement data, the public and private key must match.

- Without decryption, encrypted files cannot be read.
- Digitally signed files can be read. A valid digital signature indicates authenticity and integrity of the file. If digitally signed files have been changed, the digital signature is invalid.

Digital signature with Meteo-40	Encryption with Meteo-40
This feature is available for Ammonit Meteo-40 data loggers purchased after 14 August 2014 with installed firmware version 1.1 (2014-08-14) or later.	This feature is available since release 1.0.1 (2014-06-10) for all Ammonit Meteo-40 data loggers.



Signing and Encryption

○ Unsigned and unencrypted

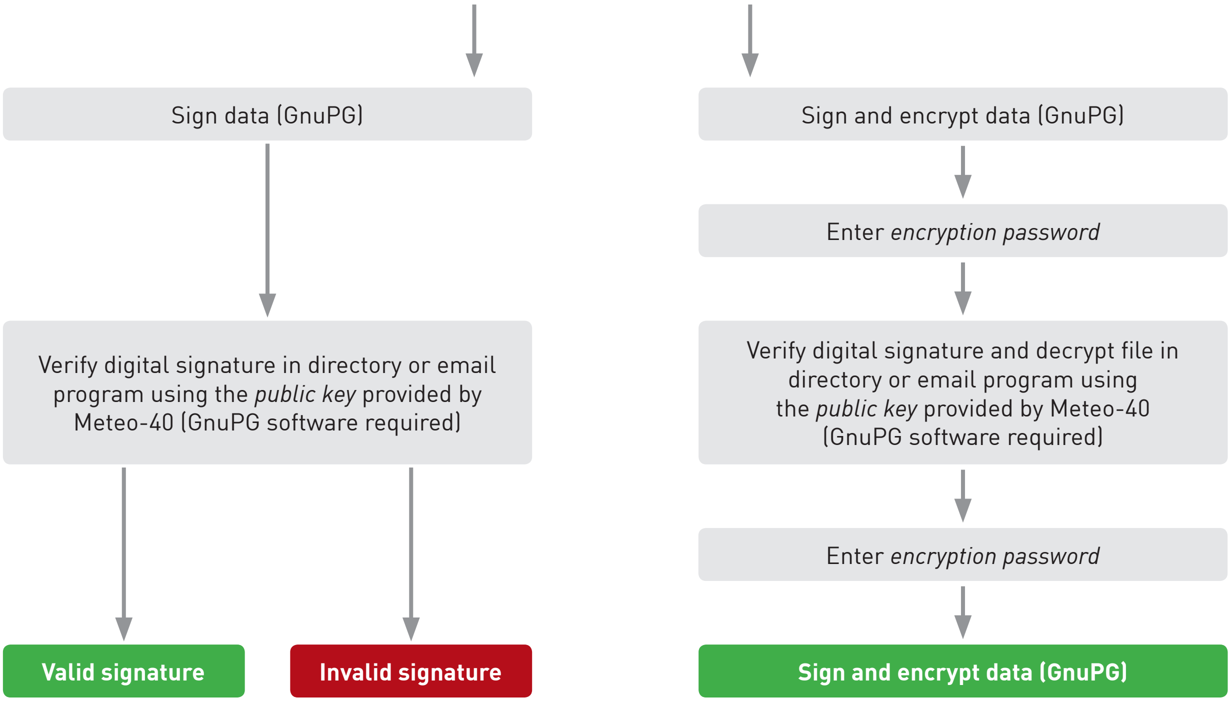
○ Sign data (GnuPG)

● Sign and encrypt data (GnuPG)

Encryption password:

•••••••• □ Show password

Fingerprint:
C41E E4BB CD80 2E08 5086 A496 BE6E A60A 4D0E 2B48



Sign data (GnuPG)

Verify digital signature in directory or email program using the *public key* provided by Meteo-40 (GnuPG software required)

Valid signature

Invalid signature

Sign and encrypt data (GnuPG)

Enter *encryption password*

Verify digital signature and decrypt file in directory or email program using the *public key* provided by Meteo-40 (GnuPG software required)

Enter *encryption password*

Sign and encrypt data (GnuPG)

Verified authenticity and integrity of the file

File has been manipulated or sender is unknown.

Only persons possessing the corresponding public key and the encryption password can read the file.

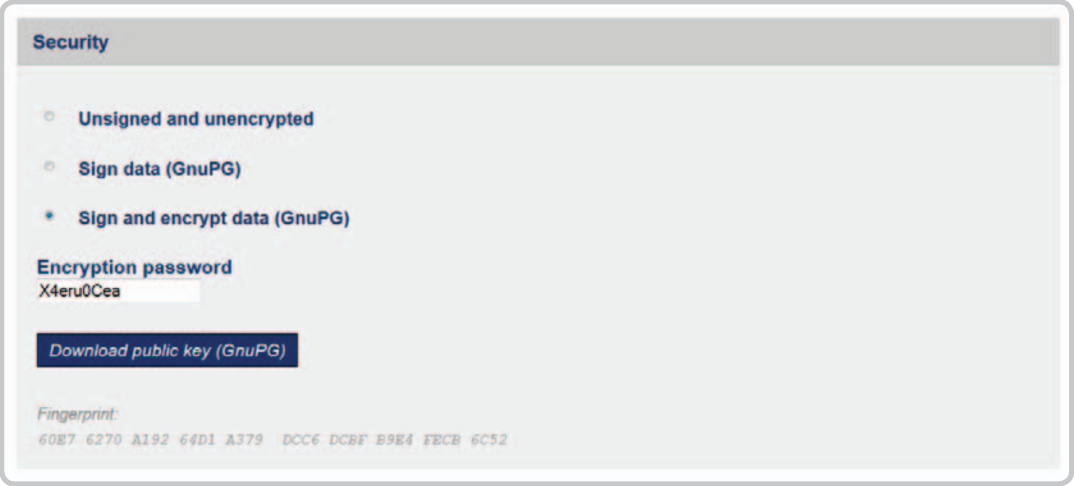
How do secure data exports work on AmmonitOR?

Protecting data exports send via email or downloaded from AmmonitOR

Each AmmonitOR installation is equipped with a unique private key. All export files sent via email or download from AmmonitOR can be encrypted and digitally signed with its individual private key. In order to verify these files, Ammonit provides a public key. To access the original export data, the public and private key must match.

- Without decryption, encrypted files cannot be read.
- Digitally signed files can be read. A valid digital signature indicates authenticity and integrity of the file. If digitally signed files have been changed, the digital signature is invalid.

Digital signature with AmmonitOR	Encryption with AmmonitOR
This feature is available for AmmonitOR installations with version 3.2.2 (2014-07-29) or later.	This feature is available for AmmonitOR installations with version 3.1.12 (2013-08-30) or later.



Security

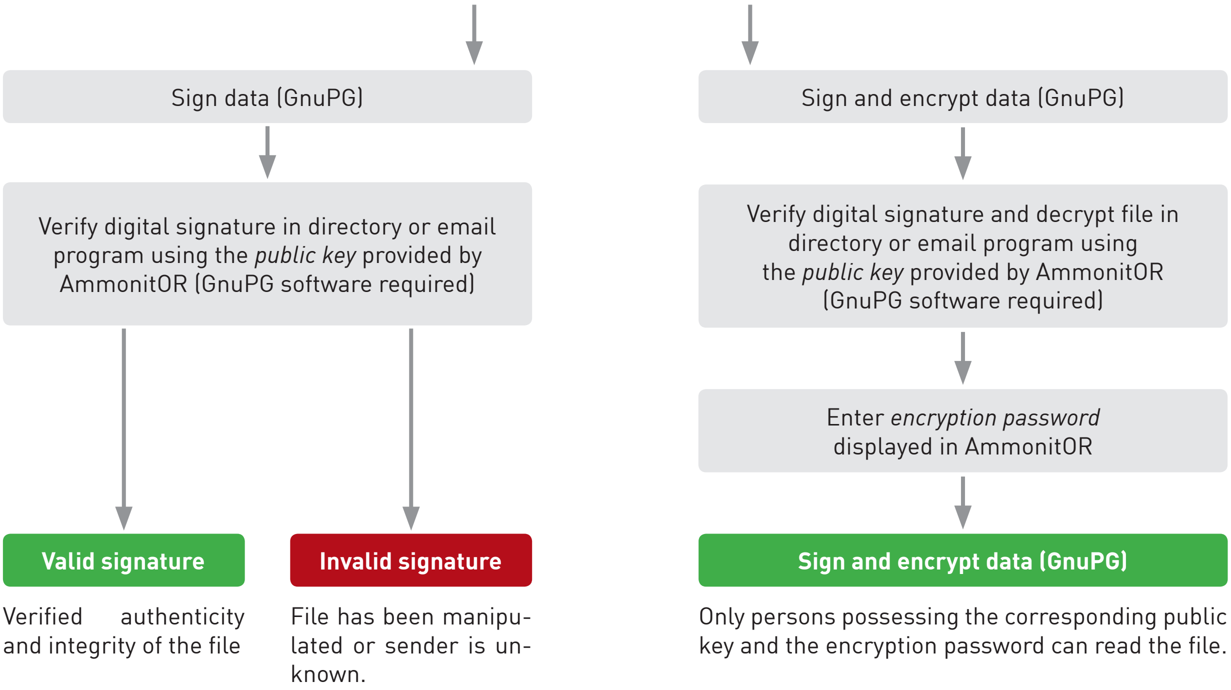
○ Unsigned and unencrypted

○ Sign data (GnuPG)

● Sign and encrypt data (GnuPG)

Encryption password
X4eru0Cea

Fingerprint:
60E7 6270 A192 64D1 A379 DCC6 DCBF B9E4 FECB 6C52



Sign data (GnuPG)

Verify digital signature in directory or email program using the *public key* provided by AmmonitOR (GnuPG software required)

Valid signature

Verified authenticity and integrity of the file

Invalid signature

File has been manipulated or sender is unknown.

Sign and encrypt data (GnuPG)

Verify digital signature and decrypt file in directory or email program using the *public key* provided by AmmonitOR (GnuPG software required)

Enter *encryption password* displayed in AmmonitOR

Sign and encrypt data (GnuPG)

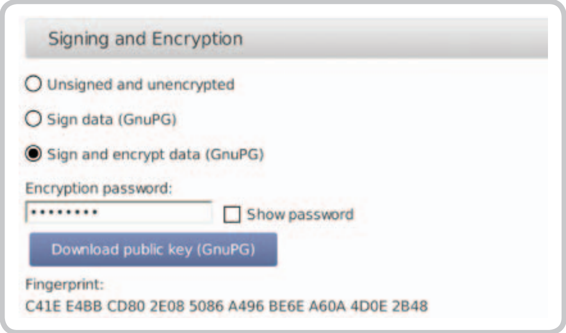
Only persons possessing the corresponding public key and the encryption password can read the file.

Requirements for verifying and decrypting files

GnuPG software

For verifying digital signatures and decrypting files, additional software is required. We recommend installing Gpg4win (GNU Privacy Guard for Windows) on Windows computers. Gpg4win needs to be configured before working with digital signatures and encryption (see scheme below).

Ammonit Meteo-40 data logger



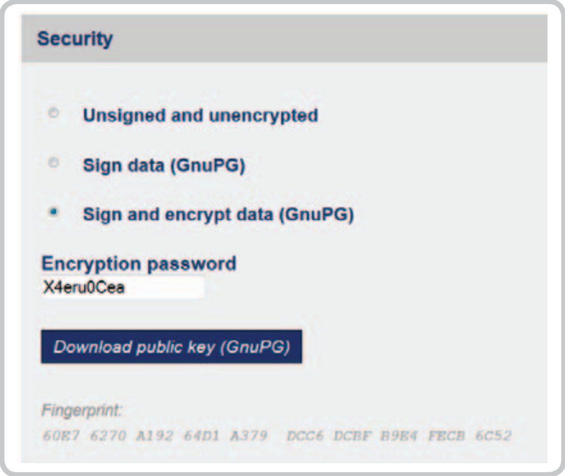
Signing and Encryption

○ Unsigned and unencrypted
○ Sign data (GnuPG)
● Sign and encrypt data (GnuPG)

Encryption password: •••••••• □ Show password

Fingerprint:
C41E E4BB CD80 2E08 5086 A496 BE6E A60A 4D0E 2B48

AmmonitOR



Security

○ Unsigned and unencrypted
○ Sign data (GnuPG)
● Sign and encrypt data (GnuPG)

Encryption password
X4eru0Cea

Fingerprint:
60E7 6270 A192 64D1 A379 DCC6 DCBF B9E4 FECB 6C52

Download *public key* (GnuPG)

Download *public key* (GnuPG)

Import *public key* in GnuPG software

Certify / verify *public key* in GnuPG software

Verify *Fingerprint* of Meteo-40 data logger with displayed *Fingerprint*

Verify *Fingerprint* of AmmonitOR installation with displayed *Fingerprint*

Trusted certificates for verifying digital signatures and decrypting files

Each Ammonit Meteo-40 data logger has a unique private key with corresponding public key.
You have to import the public keys from <u>all</u> your Meteo-40 data loggers.

Each AmmonitOR installation has a unique private key with corresponding public key.
All projects created in your AmmonitOR installation use the same public key.

SARTELCO® SISTEMI SRL
Via Torri Bianche, 1
20871 Vimercate (MB)
Tel. +39- 039- 62905.1 Fax. +39- 039- 62905.99
e-mail sistemi@sartelco.it Web www.sartelco.it