Mnova Publications File Format (.mnpub) v1.1

1. INTRODUCTION

The Mnova publications file format allows to selected publishers to view and analyze the publication datasets with Mnova. The publishers must use a RSA key pair. The public key must be sent to Mestrelab and Mestrelab will generate a corresponding certificate file (with extension mncrt). Once the publisher receives the mncrt file, they will use their private RSA key to sign their dataset, obtaining a signature. With the signature, the certification file (mncrt) and a URL to the signed dataset a mnpub file can be composed.

Mnova will read the mnpub and will verify the dataset pointed by the URL field of the mnpub, using the public key information contained in the mnpub file file.

2. GENERAL CONSIDERATIONS

mnpub is a text file encoded with UTF-8.
The line end can be either LF (Unix) or CR LF (Windows) and it can have a maximum length of 2048 characters.

3. FORMAT

3.1 HEADER

The file starts with the mandatory header line:

----- MNOVA PUBLICATIONS FILE -----

3.2 LINE SYNTAX

The next text lines to the header line must follow the syntax:

KEY:VALUE

The KEY part cannot contain the semicolon character ':'. The VALUE member can have any valid UTF-8 character. Spaces at the beginning and end of the line, and at the beginning and end of KEY and VALUE are ignored, so the line:

```
KEY :    VALUE
```

would be equivalent to the previous one and valid.
Empty lines are skipped.

3.3 CONTENTS

For the current version the predefined KEY values are:

- ? PUBKEY (mandatory)
- ? PUBKEY_ID (optional)
- ? PUBKEY_SIGN (mandatory)
- ? SIGNATURE (mandatory)
- ? URL (mandatory)

3.3.1 PUBKEY

This field is mandatory and it contains the public key used to sign the data pointed by the URL field.
The PUBKEY will be generated from the publisher's public key by Mestrelab and sent back to the publisher in the certificate file (mncrt file).

3.3.2 PUBKEY_ID

It contains the public key ID and the field is not mandatory. It identifies the ID given by Mestrelab to the publisher's public key.
The PUBKEY_ID it will be generated from the publisher's public key by Mestrelab and this is sent back to the publisher in the certificate file (mncrt file).

3.3.3 PUBKEY_SIGN

This field is mandatory and it contains the public key signature used to verify that the public key of the publisher was granted by Mestrelab.
The PUBKEY_SIGN will be generated from the publisher's public key by Mestrelab and is sent back to the publisher in the certificate file (mncrt file).

3.3.4 SIGNATURE

The signature field must exist and it will contain the signature of the file pointed by the URL field. The signature will be represented in base64 and must be in a single line. Line breaks are not allowed. For example:

SIGNATURE:M4EUJd5OpqHMt41oAIGlssLTxl52CIZZSUjHHeaIU9z5Qd2WOQtZSbfdZh50OgVfn...

NOTE: In the example above, we have truncated the signature base64 text and we are ending the field with '...' meaning that the remaining text will go there.

3.3.5 URL

The URL field must exist and it will contain either a valid URL or a relative path to the data file (relative to the mnpub file). Examples:

```
http://servername.org/path/to/file/data.zip
file:///path/to/another file/data.zip
file:///C:/windows/path/data.zip
data.zip
relative/path/data.zip
```

NOTE: As the mnpub file uses UTF-8 encoding, percent encoding for the URL value is not supported. So, the URL

http://servername.org/path%20with%20spaces/data.zip

is not supported and it should look like:

http://servername.org/path with spaces/data.zip

4. Changelog

AUTHOR	VERSION	DATE
Felipe Seoane (fseoane@mestrelab.com)	1.0	2016/02/11
David Martinsen (martinsen.david@gmail.com)	1.1	2018/12/13