H.) Format for

a) Elliptic curve parameters

The elliptic curve parameter file is a simple ascii text file printed in human readable format. It is almost self explanatory. An example parameter file contained in the standard package of Academic Signature is given below:

```
ID: anders_768_1
MODUL:
fb00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000e7
coeff_A:
fb00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000e4
coeff_B:
de5ff15ffdeadffffae5ff15ff900dfffff1ea5ff15ffbe54fffff1ea5ff15ffc001fffff1ea5ff15ff25a5afe0000000000
f0000000d672c90d27a8070266ee8fc8e4b016d9ec4f0edbef9abd2dfd1e8c429db5e2c400000000000000000185
q_MODUL:
faffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff823d
ec7f8ef180dc44c9e5cd2c1e351b51faf52779db9decc9a3e13d526b0eb2b1816ddd401d83de0dd0f3999de2fc4f
X0:
de5ff15ffdeadffffae5ff15ff900dfffff1ea5ff15ffbe54fffff1ea5ff15ffc001fffff1ea5ff15ff25a5afede5ff15ffd
eadffffae5ff15ff900dfffff1ea5ff15ffbe54fffff1ea5ff15ffc001fffff1ea5ff15ff25a5afeffffffffffff
Y0:
0559cdf3dc6b1e8e0364eb9bdac0b9b72e714c2a6e14a2cc9a188a4e6f67599b83886d1cdf4e1272f282c51b2bfee63f425f
210a7f5b80de67d1d64a19bb8f4e1739d16acf3635efc7a8ff6840f93f0d4c6e6be5298275b2bad0b84aef2dec95

 END
```

The file contains seven items preceded by a respective keyword and separated by whitespaces as defined e.g. for the C-language "scanf“ function. The items have to be arranged in the order shown in the example file.

The string following the keyword "ID: " is the identifier used to refer to this elliptic curve in Academic Signature.

The string following the Identifier "MODUL: " is the hex representation (high digit left) of the prime modulus for the underlying standard arithmetics in calculating the elliptic curve operations. All of the following hexnumbers are represented in the same way. In order to speed up modulo reductions the special value in the example file contains only zero bytes apart from the high byte and the low byte.

Keywords "coeff_A: " and "coeff_B: " denote the corresponding values of the respective parameters of the elliptic curve written in the weierstraß form:

$$y^2 = x^3 + \boldsymbol{A} \cdot x + \boldsymbol{B}$$

"q_Modul: " denotes the Group order of the respective algebraic group of the curve. In Academic Signature only curves with cofactor one should be used.

"X0: " and "Y0: " denote the point coordinate of the generator of the group.

The string "END" marks the end of the parameter set.

b) Public Keys

The public key file is a plain ascii text file printed in human readable format and is self explanatory. It should bear the filename of the key's ID with the file extension ".pell".

An example public key is given below:

```
ID_of_key: my_768_k1
Name_of_Keyholder: Michael_Anders
EllipCurve_Domain_Name: anders_768_1
Ax:
e50c765403726330ff274d70bcd37e06f6049255d95ee02059e01981ae5cb43238eb3727038fe8e8b0b9e1d5a89be356c000
b5726e6034870aa2e57e7aafc1a8d6bf0701b54d0fc165ee5272e5eb9a4d27e521cf4a033549e4d6f5d3dd843ff5
Ay:
d7385d74306950d717be9f9ea194e1c90337b63932e0dbb110477ae34a5007ca2477dd3c577d56a859e982d21e300ee72af7
847944b0aedc79f18ef6ad525fc7077b1de9806a3ab5440e4aad8c81db4cd6b59ff233e6c598291e4ae9e3222f55
```

The file contains five items preceded by a respective keyword and separated by whitespaces as defined e.g. for the C-language "scanf“ function. The items have to be arranged in the order shown in the example file.

"Ax: " and "Ay: " stand for the coordinates of the point on the elliptic curve which comprise the public key. All other identifiers should be obvious.

c) private Keys

The private key file is a symmetrically enciphered plain ascii text file printed in human readable format and is self explanatory. In deciphered form it bears the filename of the key's ID with the file extension ".prv". Unless Academic Signature is interrupted in a debugging session it is visible only in its enciphered form with the extension ".ciph". The cipher file is preceded by a plain header giving algorithm identifier, salt and stretching parameters.

The example public key file corresponding to the public key printed above is given below in deciphered form:

```
id: my_768_k1
fullnam: Michael_Anders
domnam: anders_768_1
d:
eacb7deb42e312dee8690fbb40504f450c161ad87d12d8e9f217f8ca504716a1f6980f9371800d742e950cc9960faa9c031d
467d40e51208c4bc774e08a4b6ae620584821aeef9ae0249b23a7d0ce5853bc494c7f4b6aadaf352582365f7a6b5
```

The file contains four items preceded by a respective keyword and separated by whitespaces as defined e.g. for the C-language "scanf“ function. The items have to be arranged in the order shown in the example file.

"d: " stands for the hex value of the private key. All other identifiers should have obvious meaning. Note that the value of the private key is still not given in the clear here. It had been doubly enciphered. This second layer of enciphering is only lifted in memory for a short time.