A.) Specifications of „Academic Signature – ECDSA“

Academic Signature follows the ECDSA Standard as found in many of the references referred to e.g. in the wikipedia pages.

Exceptions:

1.) The standard requires that the hash value be truncated if of higher bit size than group order.

Quote from Wikipedia:

„Let z be the L_n leftmost bits of the hash value, where L_n is the bit length of the group order n“

In Academic Signature the hash value is not truncated but interpreted as a longnumber, low byte at the start address, and then modulo reduced with respect to group order. This is to remove ambiguities when non NIST curves are used.

Rationale: Non NIST curves do not have series of 0xff as high bytes in the group order and thus the truncated hash value may correspond to a larger longnumber than n. The treatment of this case in the conventional standard is considered awkward by the author of Academic Signature and might give rise to ambiguities. Thus this part of the standard is not adopted.

2.) Academic Signature does not restrict the use of hash algorithms. If the user decides so, a hash algorithm of smaller bit length than the group order may be selected. This is to allow the use of conventional small bit size hash algorithms like SHA512 with large group order domains. (Note: Such domains up to 1024 bit group order have been developed for use in Academic Signature.)

3.) Academic Signature allows the use of new hash algorithms developed for Academic Signature with greatly increased bit size on the order of kilobytes.

4.) Some legacy checks, that only make sense for cofactor different from 1 have been omitted in Academic Signature. No one uses domains with cofactors other than 1 nowadays, so the checks for correct subgroup do not make sense.

Format and contents of the signature file:

The signature file is a simple ascii text file printed in human readable format. It is self explanatory. An example signature file is given below:

```
Domnam: p256r1
 r: a24469927a4cea5981126d105866b6d455c7206b6b5c47a51053cbac7c7d36c2
 s: 5ad7a75ababd3b25ce00dd76e50972d83e6df4667462a9cd5cca651537421044
Hash: Fleas_lb
```

The file contains four items preceded by a respective keyword and separated by whitespaces as defined e.g. for the C-language „scanf“ function.

Item one preceded by the keyword “Domnam: “ is the identifier of the elliptic curve used in the calculations.

“r: “ and “s: “ are the keys for the parameters of the signature as used in the literature. The values of the parameters are to be printed in plain hex representation(high digits left).

The key “Hash: “ precedes the identifier of the used hash algorithm. Presently these include: sha2, sha4, Fleas_lx3, Fleas_lb, Fleas_lc, Fleas_ld.

The parameters must be given in the order shown in the example signature file.

The signature file itself shall not contain a reference to the signer key. It shall have the same filename as the signed file plus the additional extension “.ecsg” and should accompany the signed file(i.e. reside in the same folder). Reference to the signer key shall solely be given in the signed document itself and be manually referred to by the verifier during the verification process.