Selene Implementation

1. Mathematical Symbols

g	g is a generator of the $q-order$ cyclic group of $GF(p)^*$ that is, an element of order q in the multiplicative group of GF(p)
P	A prime number that defines the Galois Field GF(p) and is used as a modulus in the operations of GF(p).
q	A prime factor of $p-1$.
x	An ECDSA private key
y	An ECDSA public key
(L , N)	The associated pair of length parameters for a DSA key pair, where L is the length of p, and N is the length of q.
L	The length of the parameter p in bits.
N	The length of the parameter q in bits.

2. Key Generation

In Selene, there are several keys need to be generated prior to any election. Those keys include: voter's signature keys , encryption key, voter's trapdoor keys.

The following process is used to generate voter's signature key pairs, election key pairs, and voter's trapdoor keys(PK_i):

Input:

(p, q, g) The subset of the domain parameters that are used for this process. p, q and g shall either be provided as integers during input, or shall be converted to integers prior to use. **len**(p) = 3072 bit, and **len**(q) = 256 bit.

Output:

1. *status* The status returned from the key pair generation procedure. The status will indicate SUCCESS or an ERROR

2. *(x, y)* The generated private and public keys. If an error is encountered during the generation process, invalid values for x and y should be returned. x and y are returned as integers. The generated private key x is in the range [1, q–1], and the public key is in the range [1, p-1].

Process:

1. N = **len**(q); L = **len**(p).
2. If the (L, N) pair is invalid, then return an **ERROR** indicator, Invalid x, and Invalid y.
3. Convert $returned-bits$ to the (non-negative) integer c (see Section 3).
4. x = (c mod (q - 1)) + 1.
5. y = g^x (mod p)
6. Return **SUCCESS**, x, and y.

3. Conversion of a Bit String to an Integer

All generation methods require the use of an approved, properly instantiated random bit generator (RBG). An n-long sequence of bits $x_1, ..., x_n$ is converted to an integer by the rule:

$$\{x_1, ..., x_n\} \rightarrow (x_1 * 2^{n-1}) + (x_2 * 2^{n-2}) + ... + (n_1 * 2) + x_n. \quad (1)$$

Note that the first bit of a sequence corresponds to the most significant bit of the corresponding integer, and the last bit corresponds to the least significant bit.

Input:

1. $b_1, b_2, ..., b_n$ The bit string to be converted.

Output:

1. C The requested integer representation of the bit string.

Process:

1. Let $(b_1, b_2, ..., b_n)$ be the bits of b from leftmost to rightmost.

2. $C = \Sigma_{i=1}^{n} 2^{n-1} b_i$.

3. Return C.

In this Standard, the binary length of an integer C is defined as the smallest integer n satisfying $C < 2^n$.