Claims

1. Method for operating a medical system ~~(1)~~ having a remote control device ~~(2)~~, a security module ~~(3)~~, and a medical device ~~(4)~~, the method comprising:
   - providing a pair of keys for asymmetric cryptography, the pair of keys comprising a public key and a private key, wherein the public key is provided in both the remote control device ~~(2)~~ and the medical device ~~(4)~~, and the private key is provided in the security module ~~(3)~~;
   - in the remote control device ~~(2)~~, generating an encrypted control command encrypted by applying the public key to a control command configured to control operation of the medical device ~~(4)~~;
   - receiving the encrypted control command in the security module ~~(3)~~;
   - in the security module ~~(3)~~, decrypting the encrypted control command by applying the private key, the decrypting comprises determining that the control command was encrypted by applying the public key;
   - in the security module ~~(3)~~, generating a security module encrypted control command by applying the private key to the decrypted control command or an amended medical control command derived from the decrypted control command and configured to control operation of the medical device ~~(4)~~;
   - receiving the security module ~~(3)~~ encrypted control command in the medical device ~~(4)~~;
   - in the medical device ~~(4)~~, decrypting the security module encrypted control command by applying the public key; and
   - controlling operation of the medical device ~~(4)~~ according to one of the control command and the amended control command, if the control command or the amended control command has been confirmed by a user confirmation input received in one of the security module ~~(3)~~, and the medical device ~~(4)~~.

2. Method of claim 1, wherein the generating of the security module encrypted control command further comprises:
   - applying a command security check for the encrypted control command, comprising determining whether the control command is a control command approved for remote control of the medical device ~~(4)~~ according to approved command control information provided in the security module ~~(3)~~; and
   - generating the security module encrypted control command, if the control command is determined an approved control command.

3. Method of claim 1 or 2, wherein the generating of the security module encrypted control command further comprises:
   - applying an error-detecting check for the encrypted control command, comprising determining whether the control command was correctly encrypted by the remote control device ~~(2)~~; and
   - generating the security module encrypted control command, if the control command was correctly encrypted.

4. Method of at least one of the preceding claims, wherein the generating of the security module encrypted control command further comprises:
   - applying a device security check for the encrypted control command, comprising determining whether the control command is received from a remote control device approved for remote control of the medical device ~~(4)~~ according to approved device control information provided in the security module ~~(3)~~; and
   - generating the security module encrypted control command, if the remote control device is determined to be an approved remote control device.

5. Method of at least one of the claims 2 to 4, further comprising, in the medical device ~~(4)~~, applying for the security module encrypted control command at least one of the command security check, the error-detecting check, and the device security check.

6. Method of at least one of the preceding claims, wherein the providing of the pair of keys for asymmetric cryptography comprises providing the private key in a read only data memory in the security module ~~(3)~~.

7. Method of at least one of the preceding claims, further comprising providing the security module ~~(3)~~ as a device component in one of the remote control device ~~(2)~~, and the medical device ~~(4)~~.

8. Method of at least one of the claims 1 to 6, further comprising providing the security module ~~(3)~~ as a portable device separated from the remote control device ~~(2)~~, and the medical device ~~(4)~~.

9. Method of at least one of the preceding claims, wherein the confirming of the device control command or the amended control command comprises
   - outputting command user information through an output device of a user interface provided on at least one of the remote control device ~~(2)~~, the security module ~~(3)~~, and

the medical device ~~(4)~~, the command user information being indicative of the device control command or the amended device control command; and

- receiving the user confirmation input through an input device of the user interface.

10. Method of at least one of the preceding claims, wherein the controlling of the operation further comprises controlling operation of a medical device ~~(4)~~ selected from the following group: medical pump device, insulin pump, and blood sugar measurement device.

11. A medical system ~~(1)~~, comprising the following system components

- a remote control device ~~(2)~~;
- a security module ~~(3)~~; and
- a medical device ~~(4)~~;

the system components configured to

- provide a pair of keys for asymmetric cryptography, the pair of keys comprising a public key and a private key;
- provide the public key in both the remote control device ~~(2)~~ and the medical device ~~(4)~~;
- provide the private key in the security module ~~(3)~~;
- in the remote control device ~~(2)~~, generate an encrypted control command encrypted by applying the public key to a control command;
- receive the encrypted control command in the security module ~~(3)~~;
- in the security module ~~(3)~~, decrypt the encrypted control command by applying the private key, the decrypting comprises determining whether the control command was encrypted by applying the public key;
- in the security module ~~(3)~~, generate a security module encrypted control command by applying the private key to the decrypted control command or an amended medical control command derived from the decrypted control command and configured to control operation of the medical device ~~(4)~~;
- receive the security module ~~(3)~~ encrypted control command in the medical device ~~(4)~~;
- in the medical device ~~(4)~~, decrypt the security module encrypted control command by applying the public key; and
- control operation of the medical device ~~(4)~~ according to one of the control command and the amended control command, if the control command or the amended control command has been confirmed by a user confirmation input received in one of the security module ~~(3)~~, and the medical device ~~(4)~~.

12. Medical system ~~(1)~~ of claim 11, wherein the remote control device ~~(2)~~ is a portable control device.

13. A security module for a medical system ~~(1)~~, comprising

- a data memory comprising a private key assigned to a pair of keys for asymmetric cryptography, the pair of keys comprising the private key and a public key;
- one or more data processors; and
- a data communication interface for data communication with a remote control device ~~(2)~~ and a medical device ~~(4)~~;

wherein the one or more data processors are configured to

- receive, from the remote control device ~~(2)~~, an encrypted control command encrypted by applying the public key to a control command configured to control operation of the medical device ~~(4)~~;
- decrypt the encrypted control command by applying the private key, the decrypting comprises determining whether the control command was encrypted by applying the public key;
- generate a security module encrypted control command by applying the private key to the decrypted control command or an amended medical control command derived from the decrypted control command and configured to control operation of the medical device ~~(4)~~;
- transmit the security module encrypted control command to the medical device ~~(4)~~.