

CLAIMS

1. A method of programming and authenticating a device (1) by a system (10), characterized in that it comprises:
 - receiving device information of a device (1) into a memory (4) managed by a Root-of- Trust, RoT (2), of the device (1) during device production (101),
 - bootstrapping the device (1) to the system (10), and
 - providing information on the RoT (2) and the device information for authenticating the RoT (2) by cryptographic protocols of the system (10) resulting in a binding between the authenticated RoT (2) and the device information known to the system (10), and for verifying the device production (101) of the device (1) resulting in the binding being verified by the system (10).
2. The method according to claim 1, characterized in that the device (1) has one or multiple System on a Chip, SoCs (3), and the RoT (2) manages the programming of device information for each SoC (3).
3. The method according to claim 2, characterized in that the RoT (2) is not embedded into any one of the SoCs (3) of the device (1).
4. The method according to claim 3, characterized in that the RoT (2) agrees a dedicated binding key with each SoCs (3) of the device (1) during device production (101), used to cryptographically bound the RoT (2) and the device (1).
5. The method according to claim 4, characterized in that the device key is used to encrypt the communication between the device (1) and the RoT (2).
6. The method according to any one of the preceding claims, characterized in that the RoT (2) is configured to bootstrap to the system (10) only once.
7. The method according to any one of the preceding claims, characterized in that it further comprises: reporting information on device production (101) of the RoT (2) to the security owner (11).

8. The method according to claim 7, characterized in that verification of the device production (101) of the device (1) includes verifying whether the bootstrapped RoT (2) was reported during device production (101).
9. The method according to claims 7 or 8, characterized in that the verification is forced during the bootstrap of the device (1) to the system (10).
10. The method according to any one of the claims 7 – 9, characterized in that the bootstrapped information and the reported information on device production (101) is reported to a security owner (11) of the RoT (2).
11. The method according to any one of the preceding claims, characterized in that the information on the RoT (2) consists of the public id of the RoT (2).
12. A device (1) comprising a processor, characterized in that the processor is configured to perform the steps of the method according to any one of the claims 1-11.
13. A device (1) comprising an integrated circuit, characterized in that the integrated circuit is configured to perform the steps of the method according to any one of the claims 1-11.
14. A computer program product, implemented on a computer-readable non-transitory storage medium (1), characterized in that the computer program product comprises computer executable instructions which, when executed by a processor, cause the processor to carry out the steps of the method according to any one of the claims 1-11.
15. A computer-readable non-transitory storage medium (1) characterized in that it comprises computer executable instructions which, when executed by a processor, cause the processor to carry out the steps of the method according to any one of the claims 1-11.