CLAIMS

1. A device comprising:

a PUF module comprising a physically unclonable function, PUF, and internal PUF interface logic arranged to receive an input challenge and output an output response being a deterministic function of the input challenge, the deterministic function comprising the PUF; and

one or more outer layer components providing at least part of an unsecured channel for inputting the input challenge to the internal interface logic of the PUF module and receiving back the output response output by the internal interface logic;

wherein at least one of the outer layer components is susceptible to manipulation of the input challenge and/or output response by a malicious process, but the PUF module, including the internal PUF interface logic, is encapsulated within a housing of the device and separated from the one or more outer layer components, and is thus protected from manipulation by the malicious process; and

wherein the internal PUF interface logic comprises a logging mechanism arranged to automatically log a record of the input challenge and/or output response in a log medium.

2. The device of claim 1, wherein the internal interface logic is implemented partially or wholly in firmware run on a processor of the device, wherein the firmware is stored partially or wholly in read only memory, ROM, or a secure kernel.

3. The device of any preceding claim, wherein the internal interface logic is implemented in fixed-function hardware circuitry.

4. The device of any preceding claim, wherein the at least one outer layer component comprises an external interface for receiving the input challenge from a source external to the device and/or supplying the output response to a destination external to the device, the malicious process to which the at least one outer layer component is susceptible comprising interception and manipulation of the input challenge and/or output response between the source and the external interface.

5. The device of claim 4, wherein the device comprises a dedicated PUF device.

6. The device of any of claims 1 to 4, wherein the at least one outer layer component comprises an application running on a processor within the housing of the device, wherein the application is configured to generate the input challenge, the malicious process to which the at least one outer layer component is susceptible comprising malware being run on the same processor as the application to manipulate the input challenge.

7. The device of claim 6, wherein the internal interface logic is arranged to run on either:

- a separate processor than the application; or

- the same processor as the application but in a privileged domain of a secure processor, whereas the application runs in an application domain.

8. The device of claim 6 or 7, wherein the device comprises an event data recorder, EDR, and the application comprises an EDR application.

9. The device of claim 8, wherein the application is configured to generate a result of a system which the EDR is configured to monitor, and the EDR is configured to record the result and a tag mapping the output response to the result.

10. The device of claim 9, wherein the tag comprises: a cryptographic signature generated by signing the result with the output response; or a hash-based message authentication code, HMAC, generated as a function of the result and the output response.

11. The device of claim 9 or 10, wherein the input challenge comprises meaningful data used by the application, representing a state of the system being monitored.

12. The device of claim 11, wherein the result is dependent on said data.

13. The device of any of claims 8 to 12, wherein the EDR is an EDR for a vehicle, the system which the EDR is configured to monitor comprising a system of the vehicle.

14. The device of any preceding claim, wherein the one or more outer layer components are implemented in the same housing as the PUF module.

15. The device of any preceding claim, wherein the log medium comprises a local memory of the device.

16. The device of claim 15, wherein said local memory is a tamperproof memory, write-once memory, and/or embedded in the interface logic.

17. The device of any preceding claim, wherein the log medium in which the PUF interface logic is configured to log the record comprises: a publicly accessible medium external to the device.

18. The device of claim 17, wherein the publicly accessible medium in which the PUF interface logic is configured to log the record comprises: a blockchain.

19. The device of any preceding claim, wherein the internal PUF interface logic is configured to perform the logging of the record in real-time in response the inputting of the individual input challenge.

20. The device of any preceding claim, wherein the internal PUF interface logic is configured to periodically log any input challenges received and/or output responses generated during each instance of a periodic window of time.

21. The device of claim 17 or any subsequent claim as dependent thereon, wherein the logging mechanism is configured to log the record to the publicly accessible medium in real-time in response to the inputting of the individual input challenge.

22. The device of any preceding claim, wherein logging mechanism is configured to output the record, for the logging thereof, in a packet that further comprises a signature

generated based on a cryptographic key of the logging mechanism applied to at least part of the packet comprising the record.

23. The device of claim 22 as dependent on at least claim 18, wherein the packet comprises a blockchain transaction, the record being included in an output of the blockchain transaction and the signature being included in an input of the transaction.

24. A method of using the device of any preceding claim, the method comprising:

after the record of the input challenge and/or output response has been logged in said log medium, inputting a candidate challenge to the device via the unsecured channel of the outer layer in order to cause the PUF module to generate a candidate response and return the candidate response to via the unsecured channel;

checking for evidence of manipulation by checking the candidate challenge against record of the original input challenge logged in the log medium, and/or by checking the candidate response against the record of the original output response logged in the log medium.

25. A computer program embodied on a non-transitory computer-readable medium and configured so as, when run on one or more processors, to perform the method of claim 24.