# PATENT APPLICATION

# Topologically Protected Recording Device with Sectored Architecture and Multi-Stage Signature Chain

## TECHNICAL FIELD

The present invention relates to a recording device for generating tamper-resistant audiovisual data, in particular a recording device having a sectored architecture in which a proprietary first sector and an open second sector are unidirectionally connected by a physical data diode, as well as associated methods and platform systems for authenticity verification.

## BACKGROUND OF THE INVENTION

### Problem Statement

Due to the rapid advancement of generative artificial intelligence, humans are increasingly unable to distinguish genuine recordings from AI-generated images, videos, or audio content. Deepfake technologies enable the creation of photorealistic content that is virtually indistinguishable from authentic recordings. This poses a fundamental threat to trust in visual and audiovisual media, with severe implications for journalism, war reporting, surveillance, the administration of justice, and societal communication.

### Prior Art

Known approaches include:

In-Camera Signing (Sony Camera Authenticity Solution, C2PA): Sony implements an in-camera digital signature based on the C2PA standard, in which a signature is generated and embedded in the image at the time of capture. The keys are stored in a hardware chipset. Additionally, 3D depth information is used for detection of screen re-recordings. However, the architecture is monolithic: a single security domain encompasses all cryptographic functions, without topological separation between the manufacturer domain and the user domain.

Blockchain-Embedded Camera Systems (Columbia University, WO2019236470A1): This system combines a digital camera with a hardware security module (HSM) and blockchain-enabled hardware. Hashes of the audiovisual material are published via smart contracts on a public blockchain. GPS data and spectral analysis serve for location and time verification. This system, too, is monolithically constructed and does not feature sectorization. Tamper protection is achieved through a physical tamper detection box and GPIO-based detection of unauthorized connections.

Multi-Stage Signature Chains Across Separate Devices (Skydio, US12231575B2): Skydio describes an architecture for Trusted Contextual Content (TCC), in which multiple physically separate devices—for example, a drone and its controller—each generate their own signatures and chain them together. Each device signs the entire data package accumulated up to that point, including prior signatures. However, the signatures are distributed across separate physical devices, not across topologically isolated sectors within a single recording device. A unidirectional hardware data diode between the signing instances is not provided.

PUF-Based Key Generation in Image Sensors: It is known to integrate Physical Unclonable Functions (PUFs) in image sensors to generate unique cryptographic keys from manufacturing-related variations (US11652649B2, US11316705B1). However, these approaches are limited to single-device architectures and do not combine PUF with a sectored dual-signature architecture.

Data Diodes: Hardware-based unidirectional data transmission systems are known in the field of IT/OT security. They are employed in critical infrastructures for network segregation. Their use within a recording device for topological separation of cryptographic domains is, however, not known.

Further Individual Aspects of the Prior Art: LegitIPix (US10439821B2) describes direct signature embedding in pixel data of a CMOS sensor using a shared-key approach. NXP (US20250202718A1) discloses an eIDAS-based certificate provisioning via a provisioning device. Amazon (US11770260B1) teaches a frame-by-frame hash chain for video verification. Basler (US20210385408A1) discloses an authentication module for sensor data with steganographic modification. EP3262782B1 describes an anti-tamper system with decoupled architecture and zeroization.

What the known solutions have in common is that they feature a monolithic security architecture in which a single trust domain encompasses both the sensing elements and the entire cryptographic processing. This means that the manufacturer or a single attacker with access to this trust domain can potentially compromise the entire system. There is therefore a need for an architecture that substantially increases tamper resistance through topological separation and physically enforced unidirectionality.

## SUMMARY OF THE INVENTION

The invention solves the stated problem by means of a recording device having a sectored architecture, comprising:

- a first sector (proprietary sector), assigned to the manufacturer, containing at least one image sensor and a first signature engine, wherein the data obtained from the image sensor are signed close to the source;
- a second sector (open sector), assigned to the user, containing at least a second signature engine;
- a data diode disposed between the first and the second sector, which ensures a physically enforced unidirectional data transmission from the first to the second sector;

wherein in the first sector, cryptographic hash values of the captured audiovisual signal are generated and encrypted with a private key of the first sector, and wherein the audiovisual signal together with the first signature is unidirectionally communicated to the second sector, in which a second signature is generated.

## DETAILED DESCRIPTION

The invention is described below by way of example with reference to a video camera. This example is non-limiting; the concept is transferable to all recording devices, including audio recorders, surveillance cameras, body cameras, and smartphones.

### 1. Sectored Architecture

### 1.1 First Sector (Proprietary Sector)

The first sector is attributable to the manufacturer of the recording device and is preferably configured in a manner that is as manufacturer-specific as possible. It is preferably arranged wholly or partially within the housing of the recording device, and for example wholly or partially within the second sector. Within the first sector there are located at least:

- an image sensor for capturing visual data;
- optionally further sensors, in particular microphones for capturing acoustic data;
- a first signature engine which generates cryptographic hash values from the audiovisual signal and encrypts these with a private key of a key pair assigned to the first sector.

The protection of the first sector is achieved primarily through secrecy and manufacturer-specific design. Preferably, the first signature engine is implemented as a system-on-chip (SoC) directly on the chip of the image sensor, in order to minimize the path between data source and signing point.

The signing is performed close to the source. Preferably, not only the raw data delivered by the image sensor and any microphones, but also metadata generated in the first sector—in particular autofocus information, depth sensor data, liveness parameters, and/or other sensor data of the first sector—are included in the hash value computation and signed therein jointly before leaving the first sector. Preferably, the cryptographic hash values are determined on a per-frame basis.

### 1.2 Second Sector (Open Sector)

The second sector is attributable to the user of the recording device. In contrast to the first sector, protection is achieved here not through secrecy, but through maximum transparency. Preferably, the second sector is configured as an open-source system whose hardware and software are publicly viewable and verifiable. Preferably, the second sector is likewise arranged wholly or partially within the housing of the recording device.

Within the second sector there is located at least a second signature engine. This receives the audiovisual signal together with the first signature of the first sector via the data diode and generates a second signature.

Preferably, in the second sector, additional metadata are added to the audiovisual signal, which are collected by means of additional sensors, in particular:

- a GPS module for position determination;
- a long-wave time signal receiver (e.g., DCF77 at 77.5 kHz) for an independent time reference;
- inertial sensors including gyroscopic sensors and accelerometers;
- additional environmental sensors.

### 1.3 Data Diode

A data diode is disposed between the first and the second sector. The term data diode is to be interpreted broadly and encompasses any device that effects a physically enforced unidirectional data transmission. The data diode may be realized in particular by:

- optoelectronic couplers (optocouplers), in which a light-emitting component in the first sector drives a photosensitive component in the second sector, without a practically usable return channel physically existing (the parasitic capacitance of the optocoupler is to be considered by a person skilled in the art, since it opens up a hypothetical possibility of back-coupling);
- fiber-optic connections with exclusively one light-transmitting unit and one light-receiving unit;
- circuits with strongly asymmetric transfer characteristics, in which signal transmission in the reverse direction is physically prevented or attenuated to such an extent that information backflow is not possible.

It is critical that at the interface between the sectors, data can flow exclusively in one direction—from the first to the second sector. Thereby, an attacker who has compromised the second sector is physically precluded from acting upon the first sector across the data diode.

## 2. Signature Chain

### 2.1 First Signature (Proprietary Sector)

In the first sector, cryptographic hash values are determined from the audiovisual signal. Preferably, this is done on a per-frame basis, i.e., for each captured individual frame a separate hash value is generated. The hash values are encrypted with the private key of the first sector, thereby generating the first signature.

It is possible to compress the recording data prior to hash value computation. This may also be done in parallel: in the first sector, a RAW stream may be generated and signed on a per-frame basis, and from the RAW stream, reversibly or irreversibly compressed streams may be generated that are likewise independently signed. The data diode then forwards both the RAW stream and the compressed streams together with their respective signatures to the second sector.

### 2.2 Second Signature (Open Sector)

In the second sector, the received data package—consisting of the already fully signed data package provided by the first sector (audiovisual data and optionally metadata of the first sector) and the first signature—together with the metadata collected in the second sector is subjected to a second signing. The second signature engine generates cryptographic hash values over the complete data package and encrypts these with the private key of the second sector.

The dual signature chain ensures that a forgery requires the compromise of both independent sectors. Since these are assigned to different trust domains (manufacturer vs. user) and are physically separated by the data diode, the tamper resistance is substantially increased compared to monolithic systems.

## 3. Key Generation and Key Management

### 3.1 PUF-Based Key Generation

In a preferred embodiment, the generation of the private keys involves a Physical Unclonable Function (PUF). A PUF exploits manufacturing-related, unavoidable variations in the semiconductor structure to generate a unique, hardware-bound entropy contribution.

The private key of each sector is preferably composed of at least two components:

- a PUF-derived component, which is obtained from the physical structure of the respective sector;
- a manufacturer-side or user-side component, which is introduced during initialization.

Through this partitioning, neither the manufacturer alone nor the user alone knows the complete private key of their respective sector. (Additional "key sources" may be added, with preference given to those where collaboration with the manufacturer or user is as unlikely as possible.) The PUF hardware itself also does not "know" the key, since it merely provides an entropy contribution. Preferably, after the PUF hardware has delivered its entropy contribution, it is irreversibly altered, which in systems based on MOS structures can be achieved by applying an otherwise impermissible gate-source voltage VGS. In this way, it can be achieved that, after initialization of the recording device, the private keys exist exclusively in volatile memories of the camera that are protected against readout, and specifically in at least two disjoint such memories (namely at least one in the first and at least one in the second sector).

### 3.2 Key Storage

The private keys are preferably held in volatile memory (e.g., SRAM) that is permanently powered by a battery. A loss of supply voltage leads immediately to the loss of the keys. In combination with the anti-tamper measures described below, comprehensive protection against physical key extraction is thereby achieved.

## 4. Tamper Protection (Anti-Tamper)

### 4.1 Gas Monitoring

In a preferred embodiment, at least the first sector of the recording device is filled with a gas, preferably an inert gas, whose pressure deviates significantly from ambient pressure. Throughout the entire service life of the recording device, the pressure and temperature of the gas are measured quasi-continuously.

A memory zeroization is triggered as soon as one of the following conditions is detected:

- an excessive rate of pressure change, indicating an opening of the housing;
- an absolute pressure that is too high or too low;
- an excessive deviation of the sensor data from the gas law, which may indicate a change in the effective sector volume (opening) or a manipulation of the sensor system itself;
- an impermissibly low temperature, in particular for protection against cold-boot attacks, in which an attacker attempts to preserve and read out the volatile memory at low temperature.

The pressure measurement is preferably temperature-compensated, in order to avoid false alarms (and consequently bricking) caused by temperature changes during normal operation. The described gas monitoring also provides protection against non-thermal data remanence attacks such as, for example, "volt boot" attacks, since it substantially impedes successful physical access to the key memory. Additionally or alternatively, monitoring of the chemical composition of the gas fills is possible, for example with electrochemical or optical sensors, wherein the exact composition of a gas fill from the manufacturer is preferably a manufacturer secret.

### 4.2 Thermal and Chemical Destruction

Preferably, upon detection of a manipulation, not only the memory contents are zeroized, but additionally a thermal destruction of the memory cells is initiated, for example by short-circuiting a battery arranged in the respective sector for maintaining the memory state. For example, the waste heat of a fuse associated with a battery may be used directly or indirectly (e.g., by igniting a reactive composite such as Nanofoil™) for thermal destruction. The fuse itself may also comprise a reactive composite ("Pyrofuze"). Thereby, the memory cells and their contents are irreversibly destroyed.

Additionally or alternatively, a destruction of the memory by chemical reaction with atmospheric constituents may be provided, which commences upon loss of housing integrity.

### 4.3 Further Tamper Protection Measures

A combination with further known forms of tamper protection is recommended, including prestressed glasses, sensor wires, conductive mesh structures, and similar means.

## 5. Metadata and Plausibility Verification

### 5.1 Long-Wave Time Signal and GPS Cross-Validation

The combination of a long-wave time signal receiver and a GPS module within the second sector is particularly advantageous. This enables an immediate plausibility check:

- Comparison of timestamps: The long-wave time signal (e.g., DCF77) provides a time reference independent of satellite navigation. A comparison with the GPS time allows detection of GPS spoofing.
- Comparison of the location defined by the GPS data with the long-wave time signal, taking into account the propagation time from the transmitter to the camera: If the location of the long-wave transmitter is known (e.g., Mainflingen for DCF77), the approximate distance to the transmitter can be inferred from the reception time and the signal propagation time, which must be consistent with the GPS location.

### 5.2 Atmospheric Environmental Signals as Fingerprints

The antenna of the long-wave time signal receiver can additionally be used to measure unpredictable natural atmospheric signals, in particular:

- VLF hiss (Very Low Frequency noise);
- sferics (electromagnetic pulses from lightning discharges);
- tweeks (dispersive long-range propagation of sferics in the Earth-ionosphere waveguide structure);
- fluctuations in the signal strength of the time signal transmitter.

During a live broadcast to the internet, it would be immediately noticeable if the VLF hiss of one camera deviates from that of similar cameras in the vicinity. This constitutes a practically unforgeable environmental fingerprint.

### 5.3 Inertial Sensors for Consistency Verification

Inertial sensors (accelerometers, gyroscopic sensors) in the second sector capture the motion of the recording device. By comparing the camera motion with the image content, plausibility can be verified: if the camera rotates but the image remains stable (or vice versa), this indicates a manipulation.

## 6. Anti-Screen-Recording (Protection Against Screen Re-Recording)

A further aspect of the invention relates to protection against re-recording of forged images or videos, where even lens attachments with built-in displays would be conceivable. Against this, the following are proposed in particular:

- depth sensors, wherein preferably existing autofocus systems are incorporated;
- multiple systems, in particular also those with active object illumination;
- systems that interact with the object to be recorded via ultrasound;
- liveness sensors, in particular for recording of humans.

The image sensor itself may serve as a liveness sensor if it is configured as a 4-channel sensor (RGB-IR sensor). Otherwise, an additional infrared-sensitive image sensor may be provided. Their data are not only used for color correction but are treated as part of the recording.

Signals from the above-mentioned sensors are fundamentally accorded the same significance as those from the image sensor and the microphones, and they are likewise signed close to the source. In this context, imaging sensors are preferably assigned to the first sector, while illumination means are assigned to the second sector.

## 7. Blockchain Registration and Platform Integration

### 7.1 Publication of Public Keys

The manufacturer publishes the public key of the first sector in a practically unforgeable manner, in particular in a blockchain, wherein metadata of the camera, in particular a digital fingerprint of its first sector, may be associated with the public key.

The user is enabled to likewise publish the public key of the second sector (comprising the open-source signature engine) in the blockchain, and to unambiguously cryptographically link it with the public key of the manufacturer.

### 7.2 Authenticity Verification

For authenticity verification, both encrypted hash values can then be decrypted with the deposited public keys and compared with a newly computed hash value of the audiovisual material, including metadata. The match confirms both the integrity and the authenticity of the recording.

### 7.3 Platform and Browser Integration

In a further embodiment of the invention, video platforms, social media platforms, web browsers, or browser applications are proposed which, for each uploaded purported recording (audio, video, image), verify whether it can be attributed through an unbroken certificate chain to a recording made with a recording device that performs close-to-source digital signing. The platform signals this to the user in a comprehensible manner or enables the user to preferably exclusively view recordings verified as authentic.

## 8. Further Notes on Protection Against Attacks

### 8.1 Cross-Sector Key Zeroization

Preferably, both the first and the second sector are quasi-continuously tamper-protected such that, in the case of all presumable manipulation attempts, an immediate zeroization of the respective private keys is achieved. Further preferably, a triggering of a tamper protection device in one sector even causes a zeroization of all private keys in all camera sectors, however without digital information crossing sector boundaries for this purpose. This can be achieved, for example, thermally or mechanically, in that a fuse of a battery that powers the volatile key memory in one sector inevitably co-triggers one or more corresponding fuses assigned to other sectors. For this purpose, a simply connected Al/Pd wire ("Pyrofuze") may be used, in which a first portion serves as an active fusible wire in the first sector and a second portion serves in the second and optionally further sectors; in this way, the command for key zeroization can cross a sector boundary as a diffusion-controlled chemical reaction, without an electrical or electromagnetic signal being transmitted.

### 8.2 Protection of the Data Diode

According to the invention, the only information-carrying connection between the sectors consists of one or more data diodes. Thus, the inputs and outputs of the data diodes are located in different sectors. Preferably, at least one tamper protection device of one of the sectors is configured to also detect manipulation attempts that affect the transmission path of the data diode, which may lie outside both sectors.

### 8.3 Signal Paths as Means of Manipulation Detection

In recording systems according to the invention, the image sensor is arranged within the tamper-protected first sector, which itself may lie within the second sector, and can be optically stimulated externally, while physical interference is impeded. Likewise, the signal path or paths between the image sensor and the signature engine(s) lie in a tamper-protected manner within the first sector. These signal paths can be monitored and may thus themselves form part of a manipulation detection device.

### 8.4 Inductive and Capacitive Attacks

For protection against electromagnetic attacks, it is proposed to professionally shield the sectors electromagnetically, and particularly the first sector, with appropriate filters for technically unavoidable feedthroughs. By coating at least the rear lens element of the camera with an electrically conductive layer (an ITO layer can additionally serve for reflection reduction), the first sector can form a nearly hermetic Faraday cage. If gas monitoring is employed, this lens can be connected to the sector housing via a permanent seal and must be dimensioned to permanently withstand the pressure differential between the sector pressure and the atmospheric pressure. Furthermore, to avoid common-mode interference—including deliberate interference—within the sectors, a consistently differential signal transmission may be employed, at least outside of integrated circuits. Finally, attack-vulnerable electronics may be potted, wherein the potting compound may be selected to be insoluble in organic solvents including halogenated solvents, and may contain fillers to influence its thermal conductivity (e.g., AlN) or its electromagnetic properties (e.g., ferrite powder). Further preferably, the potting compound is selected such that all solvents, including supercritical fluids, that can attack, substantially swell, or even dissolve it, can also attack and destroy the potted electronics. In addition to such passive protection, active protection is also possible here: as soon as an electromagnetic attack is detected, for example by an overvoltage event, key zeroization is triggered immediately.

### 8.5 Tamper Protection by Missing Response

Furthermore, at least in the second sector, a key zeroization can be triggered as soon as an expected signal from the data diode fails to arrive, since this may be indicative of an attack directed against the first sector. The expected signals from the data diode need not follow a regular interval, but preferably follow one another at pseudo-random intervals.

### 8.6 Permanent Cryptographic Self-Observation

In a further preferred embodiment, the recording device is configured to generate, throughout its entire operating life—including outside of regular recording operation—at preferably pseudo-random time intervals whose expected value preferably lies in the range of seconds to a few minutes, compressed background images of low resolution by means of the image sensor of the first sector. Each background image traverses the regular signature path: it is signed close to the source in the first sector, unidirectionally communicated to the second sector via the data diode, and there subjected to a second signing together with the current metadata—in particular GPS position, long-wave time signal, VLF environmental fingerprint, and inertial sensor data. Additionally, each chain element thus generated is cryptographically chained with the preceding one by including the cryptographic hash value of the preceding chain element in the subsequent one, so that a seamless, tamper-evident image chain is created over the entire service life of the device. The image chain is stored locally in the second sector in a symmetrically encrypted manner, wherein the symmetric key is known exclusively to the user. If the authenticity of a recording made with the recording device is disputed, the user can decrypt the entire image chain or—by means of a Merkle tree formed over the chain elements—a verifiable temporal section thereof and present it for review; the integrity of the chain is verifiable by seamless recomputation of the hash values, and any subsequent manipulation, insertion, or deletion of an image destroys the consistency of the chain. By keeping the image resolution sufficiently low and applying sufficiently strong data compression, such a camera can document its integrity on commercially available mass storage devices over many years. Object illumination, e.g., NIR object illumination, as per Section 6, can be incorporated into the protection concept.

## 9. PQC

Based on the strategic conjecture that NP is not a subset of BQP, in anticipation of powerful quantum computers, various new encryption and signature algorithms are being developed, so-called PQC algorithms. Preferably, at least one signature engine of the first or second sector employs a PQC algorithm. Further preferably, both the first and the second sector use signature engines with PQC algorithms, and preferably different ones, and further preferably ones that are based on different mathematical problems which cannot be efficiently reduced to one another.

## 10. Blockchain

In addition to the camera itself, a compromise of the blockchain is also conceivable, in which the public key of the manufacturer is deposited in a uniquely linked manner with that of the user. For this purpose, it is proposed to deposit these linked key pairs in a plurality of established blockchains, so that an attacker would have to simultaneously overcome the independent consensus mechanisms of a plurality of blockchains.

## 11. Powering On and Off of the First Sector

Insofar as powering on and off of the first sector is required, this is preferably done from the second sector, which preferably surrounds the first, by switching the supply voltage on and off. It is to be ensured by hardware means that no changes to the firmware in the first sector can thereby be effected.

Preferably, the firmware of the first sector distinguishes between two operating modes based on the duration of the applied supply voltage:

- In the case of a short voltage pulse whose duration is below a predetermined threshold duration, the first sector generates, after startup, a single signed image (challenge-response frame) and outputs it via the data diode to the second sector, whereupon the second sector switches the supply voltage off again.

- In the case of a supply voltage that is applied beyond the threshold duration, the first sector commences regular audiovisual recording operation.

The second sector monitors the response time of the first sector to the voltage pulse. If the expected response fails to arrive within a predetermined time window, or if the response time deviates impermissibly from a time profile characteristic of the first sector, this is evaluated as a manipulation indicator and may trigger a key zeroization in accordance with Section 8.5. The challenge-response frames generated at pseudo-random intervals are preferably incorporated into the image chain in accordance with Section 8.6. This serves to defend against side-channel attacks.

## 12. Digital Terminal Devices

The integration of recording devices according to the invention into digital terminal devices such as smartphones enables anyone to make recordings of the highest evidentiary value.

## 13. Definitions

A "sector" within the meaning of this application designates a physically delimited functional area within a single device that comprises its own processing units, its own memory, and its own cryptographic infrastructure, and that is informationally isolated from other sectors of the same device—that is, between the sectors there exists no intended or unintended information path other than the provided data diode, wherein side channels such as electromagnetic emanation, power consumption patterns, thermal coupling, or shared clock sources are suppressed by suitable design measures.

A "trust domain" is the totality of those hardware and software components whose integrity is under the control of exactly one responsible entity—such as the manufacturer or the user—and that are assigned to a common root of trust; different trust domains are characterized by the fact that none of them need presuppose the integrity of any other.

A root of trust is that component within a trust domain whose authenticity and integrity is not derived from a further entity within the same domain, but is taken as given—typically a cryptographic key or a hardware component housing such a key, from which the chain of trust for all remaining components of the domain originates.

A data diode is a physical connection between two sectors that restricts the information flow by hardware means to exactly one direction and physically prevents a backflow—unlike a merely software-based access control.

A signature engine designates a unit integrated in the respective sector that forms cryptographic hash values from received data and digitally signs these by means of a private key exclusively assigned to the sector.

Close to the source means that the signing is performed spatially and in terms of circuit design so close to the sensor that no unsecured, externally accessible signal path exists between data capture and signing.

Claims

Group A: Sectored Architecture and Data Diode (Claims 1–13)

Independent Claim 1 – Sectored Recording Device

1. A recording device for generating tamper-resistant data, comprising:

a) a first sector comprising at least one sensor and a first signature engine, the first signature engine being configured to determine, close to the source, cryptographic hash values from a signal captured by the sensor and to encrypt said hash values with a private key of a key pair assigned to the first sector, so as to generate a first signature;

b) a second sector comprising at least a second signature engine, the second signature engine being configured to receive the signal and the first signature and to generate a second signature using a private key of a key pair assigned to the second sector;

c) a data diode disposed between the first sector and the second sector, which effects a physically enforced unidirectional data transmission from the first sector to the second sector and prevents information backflow from the second sector to the first sector;

wherein the first sector and the second sector are assigned to different trust domains.

2. The recording device according to claim 1, wherein the first sector is assigned to the manufacturer of the recording device and the second sector is assigned to the user of the recording device.
3. The recording device according to any one of the preceding claims, wherein the sensor comprises an image sensor and the signal is an audiovisual signal.
4. The recording device according to any one of the preceding claims, wherein the data diode is realized by at least one of:

a) an optoelectronic coupler, in which a light-emitting component in the first sector drives a photosensitive component in the second sector;

b) a fiber-optic connection with exclusively one light-transmitting unit and one light-receiving unit;

c) a circuit with strongly asymmetric transfer characteristics, which physically prevents signal transmission in the reverse direction or attenuates it to such an extent that information backflow is prevented.

5. The recording device according to any one of the preceding claims, wherein the first sector is arranged wholly or partially within the second sector.

6. The recording device according to any one of the preceding claims, wherein the first sector is configured in a manufacturer-specific and proprietary manner and the second sector is configured as an open-source system whose hardware and/or software specification is publicly viewable and verifiable.

7. The recording device according to any one of the preceding claims, wherein the first signature engine is configured to include in the hash value computation and to sign, jointly with the sensor data, metadata generated in the first sector—in particular autofocus information, depth sensor data, and/or liveness parameters—before said data leave the first sector.

8. The recording device according to any one of the preceding claims, wherein the first signature engine is integrated as a system-on-chip (SoC) on the chip of the image sensor, so that the signal path between data source and signing point is minimized.

9. The recording device according to any one of the preceding claims, wherein in the first sector, a RAW data stream and at least one compressed data stream are generated in parallel and both data streams are independently signed before being communicated to the second sector via the data diode.

10. The recording device according to any one of the preceding claims, wherein the second sector further comprises a plurality of sensors selected from: a GPS module, a long-wave time signal receiver, inertial sensors including gyroscopic sensors and accelerometers, environmental sensors, and wherein the metadata captured by these sensors are added to the signal prior to the second signing.

11. The recording device according to any one of the preceding claims, wherein the recording device is configured to activate and deactivate the first sector by controlling the supply voltage from the second sector, it being ensured by hardware means that no changes to a firmware of the first sector can thereby be effected.

12. The recording device according to claim 11, wherein the firmware of the first sector distinguishes between at least two operating modes based on the duration of the applied supply voltage:

a) a challenge-response mode, in which upon a voltage pulse having a duration below a predetermined threshold duration, a single signed image is generated and output via the data diode; and

b) a regular recording mode, in which upon a supply voltage applied beyond the threshold duration, continuous recording operation is commenced.

13. The recording device according to claim 12, wherein the second sector monitors the response time of the first sector to a voltage pulse and evaluates a failure of

the expected response to arrive or an impermissible deviation of the response time from a time profile characteristic of the first sector as a manipulation indicator.

Group B: Key Generation and PUF Destruction (Claims 14–18)

Independent Claim 14 – PUF-Based Key Generation with Irreversible PUF Destruction

14. A method for key generation for a cryptographic system, comprising the steps of:

a) obtaining a hardware-bound entropy contribution by means of a Physical Unclonable Function (PUF) that exploits manufacturing-related variations of a semiconductor structure;

b) combining the entropy contribution with at least one further key component to generate a private key;

c) storing the private key in a volatile memory;

d) after completion of the key generation, irreversibly destroying the PUF hardware so that a renewed obtaining of the entropy contribution is physically impossible;

wherein after step d) the private key exists exclusively in the volatile memory.

15. The method according to claim 14, wherein the irreversible destruction of the PUF hardware is effected by applying a voltage to at least one MOS device of the PUF that produces an irreversible gate oxide breakdown.

16. The method according to claim 14 or 15, wherein the private key is composed of at least three components: the PUF entropy contribution, a piece of partial information introduced by the manufacturer, and a piece of partial information introduced by the user, so that neither the manufacturer, nor the user, nor the PUF hardware alone knows or can reconstruct the complete private key.

17. The method according to any one of claims 14 to 16, wherein the volatile memory is an SRAM memory that is permanently powered by a battery, and wherein a loss of supply voltage leads to the immediate and irreversible loss of the private key.

18. The recording device according to any one of claims 1 to 13, wherein in at least one of the sectors a private key is generated and stored according to the method of any one of claims 14 to 17, and wherein preferably in each of the sectors a respective private key is generated and the respective PUF is irreversibly destroyed, so that after initialization the private keys exist exclusively in volatile memories in at least two disjoint sectors.

Group C: Gas Pressure Monitoring (Claims 19–23)

Independent Claim 19 – Gas Pressure Monitoring for Tamper Detection

19. An electronic device with tamper protection, comprising:

a) at least one memory in which security-relevant data are held;

b) at least one gas-tight housing in which the memory is arranged and which is filled with a gas whose pressure deviates from an ambient pressure;

c) at least one pressure sensor and at least one temperature sensor, which measure the pressure and the temperature of the gas quasi-continuously;

d) an evaluation unit configured to trigger a zeroization of the security-relevant data as soon as at least one of the following conditions is detected:

- i) a rate of pressure change that exceeds a predetermined threshold value;
- ii) an absolute pressure outside a permissible pressure range;
- iii) a deviation between the measured pressure and a pressure expected on the basis of the measured temperature and a known volume according to the ideal gas law that exceeds a predetermined tolerance range;
- iv) a temperature below a predetermined minimum value, in particular for protection against cold-boot attacks.

20. The electronic device according to claim 19, wherein the gas is an inert gas and/or wherein the chemical composition of the gas fill is monitored by means of electrochemical or optical sensors, the exact composition being a manufacturer secret.

21. The electronic device according to claim 19 or 20, wherein the evaluation unit is further configured to initiate, upon detection of a manipulation, in addition to data zeroization, a thermal destruction of the memory, in particular by short-circuiting a battery powering the memory.

22. The electronic device according to any one of claims 19 to 21, wherein upon loss of housing integrity, a chemical destruction of the memory is provided by reaction of memory components or a reactive substance surrounding them with atmospheric constituents.

23. The recording device according to any one of claims 1 to 13 and 18, wherein at least one sector is configured as an electronic device according to any one of claims 19 to 22.

Group D: Cross-Sector Key Zeroization (Claims 24–27)

Independent Claim 24 – Key Zeroization by Diffusion-Controlled Chemical Reaction

24. An electronic device having at least two spatially separated security zones, wherein:

a) in each security zone, at least one volatile memory is arranged that contains security-relevant data and is powered by an associated battery, a fuse being associated with each battery;

b) the fuses of the different security zones are thermally coupled by at least one contiguous reactive element, the reactive element having a first portion in a first security zone and a second portion in a second security zone;

c) triggering of the fuse in one security zone initiates an exothermic, self-sustaining chemical reaction of the reactive element, which propagates along the reactive element and inevitably co-triggers the fuse of the other security zone;

so that a command for key zeroization crosses a security zone boundary as a diffusion-controlled chemical reaction, without an electrical or electromagnetic signal being transmitted.

25. The electronic device according to claim 24, wherein the reactive element comprises a wire of an aluminum-palladium alloy (Pyrofuze) or a reactive multilayer film based on aluminum and nickel (NanoFoil).

26. The electronic device according to claim 24 or 25, wherein the reactive element additionally serves as a fuse of one or more of the batteries.

27. The recording device according to any one of claims 1 to 13, 18, and 23, wherein the first and the second sector are thermally coupled according to any one of claims 24 to 26 by a reactive element.

Group E: Permanent Cryptographic Self-Observation (Claims 28–32)

Independent Claim 28 – Cryptographic Image Chain

28. The recording device according to any one of claims 1 to 13, wherein the recording device is configured to generate, throughout its entire operating life—including outside of regular recording operation—at time intervals whose expected value preferably lies in the range of seconds to a few minutes, compressed background images by means of the sensor of the first sector, wherein:

a) each background image is signed close to the source in the first sector, unidirectionally communicated to the second sector via the data diode, and there subjected to a second signing together with current metadata;

b) each chain element is cryptographically chained with the preceding one by including the cryptographic hash value of the preceding chain element in the subsequent one;

c) the resulting image chain is stored locally in the second sector in encrypted form;

so that a seamless, tamper-evident image chain is created over the entire operating life of the recording device.

29. The recording device according to claim 28, wherein the time intervals between the background images are determined pseudo-randomly.

30. The recording device according to claim 28 or 29, wherein a Merkle tree is formed over the chain elements, which enables a verifiable disclosure of a temporal section of the image chain without having to disclose the entire chain.

31. The recording device according to any one of claims 28 to 30, wherein the image chain further comprises the challenge-response frames generated according to claim 12.

32. The recording device according to any one of claims 28 to 31, wherein the image chain is stored in a symmetrically encrypted manner, the symmetric key being known exclusively to the user.

Group F: Anti-Screen-Recording and Liveness (Claims 33–34)

33. The recording device according to any one of claims 1 to 13, wherein the first sector further comprises at least one of the following systems for detection of screen reproductions:

a) a depth sensor, wherein preferably an existing autofocus system is incorporated;

b) a system with active object illumination, in particular in the near-infrared range;

c) an ultrasonic interaction system for determining three-dimensional object properties;

d) a liveness sensor, in particular an image sensor configured as an RGB-IR sensor (4-channel sensor), which simultaneously captures visible light and infrared radiation;

wherein signals from these sensors are signed close to the source in the first sector.

34. The recording device according to claim 33, wherein imaging sensors are assigned to the first sector and illumination means are assigned to the second sector, so that a compromise of the second sector does not impair the authenticity of the imaging sensors.

Group G: Electromagnetic and Chemical Protection (Claims 35–38)

Independent Claim 35 – Electromagnetic and Chemical Protection of a Cryptographic Assembly

35. An electronic assembly with cryptographic function, comprising:

a) a cryptographic circuit embedded in a potting compound, the potting compound being selected such that:

- i) it is insoluble in organic and halogenated solvents at standard conditions; and

- ii) all solvents, including supercritical fluids, that can substantially swell or dissolve the potting compound can also attack and functionally destroy the potted electronics;

b) an electromagnetic shield that at least partially surrounds the cryptographic circuit, wherein for optical feedthroughs an electrically conductive, optically transparent coating, in particular an ITO coating, is provided;

c) a consistently differential signal transmission arranged within the shield, at least outside of integrated circuits, for suppression of common-mode interference.

36. The electronic assembly according to claim 35, wherein the potting compound contains fillers for influencing its thermal conductivity and/or electromagnetic properties, in particular aluminum nitride (AlN) and/or ferrite powder.

37. The electronic assembly according to claim 35 or 36, wherein the electrically conductive, optically transparent coating is applied on the rear lens element of an objective lens and, in conjunction with a conductive housing, forms a substantially closed Faraday cage, the coating being connected to the housing via a permanent seal.

38. The recording device according to any one of claims 1 to 13, wherein at least the first sector is configured as an electronic assembly according to any one of claims 35 to 37.

Group H: Data Diode Protection and Signal Path Monitoring (Claims 39–42)

39. The recording device according to any one of claims 1 to 13, wherein at least one tamper protection device of one of the sectors is configured to also detect manipulation attempts that affect a transmission path of the data diode lying outside both sectors.

40. The recording device according to any one of claims 1 to 13, wherein at least in the second sector a key zeroization is triggered as soon as an expected signal from the data diode fails to arrive, the expected signals preferably following one another at pseudo-random intervals.

41. The recording device according to any one of claims 1 to 13, wherein at least one signal path between the sensor and the first signature engine within the first sector is monitored and a change in this signal path is evaluated as a manipulation indicator.

42. The recording device according to any one of claims 1 to 13, wherein upon detection of an electromagnetic attack, in particular an overvoltage event, an immediate key zeroization is triggered.

Group I: PQC and Blockchain (Claims 43–45)

43. The recording device according to any one of claims 1 to 13, wherein at least one of the signature engines employs a post-quantum cryptography algorithm (PQC algorithm).

44. The recording device according to claim 43, wherein the first and the second signature engine employ different PQC algorithms that are based on different mathematical problems, in particular selected from: lattice-based problems, code-based problems, hash-based schemes, and/or multivariate polynomial equation systems.

45. The recording device according to any one of claims 1 to 13, wherein the public keys of the first and the second sector are deposited in a linked manner in a plurality of mutually independent blockchains, so that an attacker would have to simultaneously overcome the independent consensus mechanisms of a plurality of blockchains.

Group J: Atmospheric Signals (Claims 46–48)

Independent Claim 46 – Authenticity Verification by Means of Atmospheric Electromagnetic Signals

46. A system for authenticity verification of a data set, comprising:

a) at least one sensor for capturing an electromagnetic environmental signal in a frequency range that reflects atmospheric propagation conditions determined by natural or large-scale technical processes, in particular in the VLF range (Very Low Frequency);

b) a processing unit configured to:

- i) determine from the captured electromagnetic environmental signal at least one characteristic parameter or feature pattern, in particular sferics, tweeks, and/or VLF hiss; and
- ii) associate the parameter or the feature pattern temporally and spatially with a recording event;

c) a comparison unit configured to:

- i) provide reference data on electromagnetic environmental signals, the reference data having been captured and aggregated by at least one reference receiver and/or by an external observation infrastructure; and
- ii) compare the determined parameter or the feature pattern with the reference data and derive from the comparison a measure of plausibility for the asserted location and/or time of the recording event;

wherein the system is configured to make, on the basis of the measure of plausibility, a statement regarding the authenticity of the data set with respect to its location and/or time specification.

47. The system according to claim 46, wherein the reference receiver is a further recording device, in particular a recording device according to any one of claims 1 to 13.

48. The system according to claim 46 or 47, wherein the external observation infrastructure comprises at least one of an Earth observation satellite, a network of geophysical sensors, or a lightning location network.

Group K: Platform System for Authenticity Verification (Claims 49–50)

Independent Claim 49 – Platform System

49. A data processing system, in particular a video platform, social media platform, web browser, or browser application, configured to:

a) verify, for a received audiovisual data element, whether it can be attributed through an unbroken certificate chain to a recording made with a recording device that has a multi-stage signature chain based on at least two independent trust domains;

b) signal to a user whether the audiovisual data element has been verified as authentic; and/or

c) enable the user to activate a filter in which preferably exclusively recordings verified as authentic are displayed.

50. The data processing system according to claim 49, wherein the verification according to feature a) comprises verifying a first signature of a proprietary sector and a second signature of an open sector against cryptographically linked public keys deposited in at least one blockchain, and wherein verification of both signatures is required for a positive authenticity assessment.