CLAIMS

1. A security marking (100) characterized by comprising:

a flat substrate (110);

a magnetically induced layer (120) of a material comprising magnetically oriented reflective platelet-shaped magnetic or magnetizable pigment particles, the magnetically induced layer being applied on the substrate (110) and comprising a first zone (120a) wherein said magnetically oriented reflective platelet-shaped magnetic or magnetizable pigment particles have their planar faces oriented in a first direction and a second zone (120b), distinct from the first zone (120a), wherein said magnetically oriented reflective platelet-shaped magnetic or magnetizable pigment particles have their planar faces oriented in a second direction distinct from the first direction, the platelet-shaped particles in the first zone (120a) having planar faces with an elevation angle γ_1 with respect to a plane of the substrate (110) and the platelet-shaped particles in the second zone (120b) having planar faces with an elevation angle γ_2 with respect to the plane of the substrate (110), each acute angle of the planar faces with respect to the plane of the substrate being in a range from 5° to 25°;

a machine readable marking (130) including a reference pattern (133) and a code pattern (134) representing encoded data, the machine readable marking (130) being respectively applied either on a top face (121) of the magnetically induced layer (120) or on the substrate (110) between said substrate and a rear face (122) of the magnetically induced layer (120), a first area (134a) of the code pattern (134) being disposed in front of the first zone (120a) and a remaining second area (134b) of the code pattern (134) being disposed in front of the second zone (120b).

2. The security marking according to claim 1, wherein

a) said pigment particles comprise:

a magnetic metal selected from the group consisting of cobalt, iron, gadolinium and nickel;

a magnetic alloy of iron, chromium, manganese, cobalt, nickel or a mixture of two or more thereof;

a magnetic oxide of chromium, manganese, cobalt, iron, nickel or a mixture of two or more thereof; or

a mixture of two or more thereof; or

b) the code pattern is any one of a one-dimensional barcode, a stacked one-dimensional barcode, a two-dimensional bar code, and a three-dimensional barcode.

3. The security marking according to any one of claims 1 and 2, wherein the first zone (120a) and the second zone (120b) of the magnetically induced layer (120) belong to a same single layer of material.

4. The security marking according to any one of claims 1 and 2, wherein the first zone (120a) and the second zone (120b) of the magnetically induced layer (120) respectively belong to a first sub-layer and an adjacent second sub-layer forming the magnetically induced layer (120).

5. The security marking according to any one of claims 1 to 4, wherein the machine readable marking (130) is applied on the top face (121) of the magnetically induced layer (120) and encoded with dark symbols and a dark primer layer (140) is applied on the substrate (110), and the rear face (122) of the magnetically induced layer (120) is applied on a top face (141) of the dark primer layer (140).

6. The security marking according to any one of claims 1 to 4, wherein the machine readable marking (130) is applied on the top face (121) of the magnetically induced layer (120) and encoded with bright symbols and a dark primer layer (140), preferably a black primer, is applied on the substrate (110), and the rear face (122) of the magnetically induced layer (120) is applied on a top face (141) of the dark primer layer (140).

7. The security marking according to any one of claims 1 to 4, wherein the machine readable marking (130) is applied on the substrate (110) and encoded with dark symbols.

8. A method for reading and decoding the security marking (100) according to any one of claims 1 to 7, with a portable device (200) equipped with a light source (201) operable to deliver illumination light, an imager (202), and a processor equipped with a memory and adapted to perform image processing and decoding operations, comprising the steps of:

disposing the security marking (100) within a field of view of the imager (202);

illuminating the security marking (100) with illumination light delivered by the light source (201);

acquiring a first digital image of the security marking (100) with the imager (202) at a first viewing angle θ_1 associated with the first elevation angle γ_1, and storing the acquired first digital image in the memory;

acquiring a second digital image of the security marking (100) with the imager at a second viewing angle θ_2 associated with the second elevation angle γ_2, and storing the acquired second digital image in the memory;

forming, via image processing with the processor, a composite digital image of the code pattern (134) from the stored first

digital image and the stored second digital image by aligning with respect to the reference pattern (133), detected in the first digital image and the second digital image, a first part of the code pattern (134) corresponding to the first area (134a) of the code pattern detected on the first digital image and a second part of the code pattern (134) corresponding to the second area (134b) of the code pattern detected on the second digital image, and storing the obtained composite digital image in the memory;

reading and decoding with the processor the code pattern (134) from the stored composite digital image.

9. A portable device (200) for reading and decoding the security marking (100) according to any one of claims 1 to 7, comprising:

a light source (201) operable to deliver illumination light;

an imager (202); and

a processor equipped with a memory,

and adapted to perform the steps of:

illuminating the security marking (100) with illumination light delivered by the light source (201);

acquiring a first digital image of the security marking (100) with the imager (202) at a first viewing angle θ_1 associated with the first elevation angle γ_1, and storing the acquired first digital image in the memory;

acquiring a second digital image of the security marking (100) with the imager at a second viewing angle θ_2 associated with the second elevation angle γ_2, and storing the acquired second digital image in the memory;

forming, via image processing with the processor, a composite digital image of the code pattern (134) from the stored first digital image and the stored second digital image by aligning with respect to the reference pattern (133), detected in the first digital image and the second digital image, a first part of the

code pattern (134) corresponding to the first area (134a) of the code pattern detected on the first digital image and a second part of the code pattern (134) corresponding to the second area (134b) of the code pattern detected on the second digital image, and storing the obtained composite digital image in the memory;

reading and decoding with the processor the code pattern (134) from the stored composite digital image.

10. A security document (150) delivered by an authority to a user, characterized by comprising:

a security marking (100) according to any one of claims 1 to 7 applied on the security document (150), wherein encoded data in the code pattern (134) of the security marking (100) contain digital identity data corresponding to the user and a digital signature of said user digital identity data, the digital signature delivered by the authority being obtained by signing the user digital identity data with a cryptographic key.

11. A method of verifying a security document (150) of a user according to claim 10, with a portable device (200) according to claim 9 further equipped with a communication unit operable to send and receive data over the communication network (CN) to a server (S) of the authority connected to a database (DB) storing the cryptographic key and a corresponding decryption key, comprising the steps of:

disposing the security marking (100) within a field of view of the imager (202);

illuminating the security marking (100) of the security document (150) with the light source (201);

acquiring a first digital image of the illuminated security marking (100) with the imager (202) at a first viewing angle θ_1

associated with the first elevation angle γ_1, and storing the acquired first digital image in the memory;

acquiring a second digital image of the illuminated security marking (100) with the imager (202) at a second viewing angle θ_2 associated with the second elevation angle γ_2, and storing the acquired second digital image in the memory;

forming, via image processing with the processor, a composite digital image of the code pattern (134) from the stored first digital image and the stored second digital image by aligning with respect to the reference pattern (133), detected in the first digital image and the second digital image, a first part of the code pattern (134) corresponding to the first area (134a) of the code pattern detected on the first digital image and a second part of the code pattern (134) corresponding to the second area (134b) of the code pattern detected on the second digital image;

reading and decoding the code pattern (134) from the composite digital image, and extracting from decoded data of the code pattern a user identity data and a digital signature of said user identity data, via image processing and decoding operations with the processor, and storing the extracted user identity data and digital signature in the memory;

sending a first message (M1) containing the extracted user identity data and digital signature stored in the memory via the communication unit (CN) to the server (S);

decrypting at the server (S) the extracted digital signature received in the first message (M1) from the portable device (200) with the decryption key stored in the database (DB), and checking whether the extracted user identity data received in the first message (M1) matches the received extracted digital signature; and

in case of matching, sending back to the portable device (200) a server message (SM) indicating a successful verification of the user identity data.

12. Method according to claim 11, comprising, prior to the step of sending back a server message to the portable device (200), the preliminary steps of:

illuminating the magnetically induced layer (120) with the light source (201) and acquiring a plurality of digital images of the illuminated magnetically induced layer (120) with the imager (202), the imager (202) being for each different digital image at a corresponding distinct viewing angle θ with respect to said magnetically induced layer (120), by moving the imager (202) relatively to the magnetically induced layer (120) parallel to the plane of the substrate (110);

for each acquired digital image, calculating, with the processor, respectively corresponding intensity I of light reflected by the magnetically induced layer (120) and collected by the imager (202) at corresponding viewing angle θ, and storing the calculated intensities of the reflected light and corresponding viewing angles to obtain a corresponding reflected light intensity curve I(θ);

sending with the communication unit a second message (M2) to the server (S) via the communication network (CN) containing the obtained reflected light intensity curve I(θ);

comparing at the server (S) the reflected light intensity curve I(θ) received in the second message (M2) with a reference reflected light intensity curve $I_{ref}(\theta)$ for said magnetically induced layer (120) stored in the database (DB);

determining at the server (S) whether the magnetically induced layer (120) is genuine based on a result of the comparison; and

in case the magnetically induced layer (120) is determined as genuine, sending back to the portable device (200) the server message (SM) indicating a successful verification of the user identity data together with an indication that the security marking

(100) is genuine, and sending by the server (S) via the communication network (CN) a server authorization message (SAM) to a communication device of the user containing access data granting to the user access to a service.

13. Method according to claim 11, comprising, in case of delivering by the server (S) of a server message (SM) indicating a successful verification of the user identity data, the further steps of:

illuminating the magnetically induced layer (120) with the light source (201) and acquiring a plurality of digital images of the illuminated magnetically induced layer (120) with the imager (202), the imager (202) being for each different digital image at a corresponding distinct viewing angle θ with respect to said magnetically induced layer (120), by moving the imager (202) relatively to the magnetically induced layer (120) parallel to the plane of the substrate (110);

for each acquired digital image, calculating, with the processor, respectively corresponding intensity I of light reflected by the magnetically induced layer (120) and collected by the imager (202) at corresponding viewing angle θ, and determining with the calculated intensities of the reflected light and corresponding viewing angles a corresponding reflected light intensity curve I(θ);

comparing via the processor the reflected light intensity curve I(θ) with a reference reflected light intensity curve $I_{ref}(\theta)$ for said magnetically induced layer (120) stored in the memory;

determining whether the magnetically induced layer (120) is genuine based on a result of the comparison, and, in case the magnetically induced layer (120) is determined as genuine, sending to the server (S), with the communication unit via the communication network (CN), a message (M) indicating that the security marking (100) is genuine; and

in case of reception at the server (S) of a message (M) from the portable device (200) indicating that the security marking (100) is genuine, sending back by the server (S) via the communication network (CN) a server authorization message (SAM) to a communication device of the user containing access data granting to the user access to a service.

14. A System for verifying a security document (150) according to claim 10 delivered by an authority to a user, comprising:

a server (S) of the authority connected to a database (DB) storing the cryptographic key and a corresponding decryption key, and operable to send and receive data via a communication network (CN); and

a portable device (200) according to claim 9 for reading and decoding a security marking (100) according to any one of claims 1 to 7 applied on the security document (150), comprising:

a light source (201) operable to deliver illumination light;

an imager (202);

a communication unit operable to send and receive data over the communication network (CN) to the server (S); and

a processor equipped with a memory and adapted to perform image processing and decoding operations, and adapted to carry out the steps of:

illuminating the security marking (100) with illumination light delivered by the light source (201);

acquiring a first digital image of the security marking (100) with the imager (202) at a first viewing angle θ_1 associated with the first elevation angle γ_1, and storing the acquired first digital image in the memory;

acquiring a second digital image of the security marking (100) with the imager at a second viewing angle θ_2 associated with the

second elevation angle γ_2, and storing the acquired second digital image in the memory;

forming, via image processing with the processor, a composite digital image of the code pattern (134) from the stored first digital image and the stored second digital image by aligning with respect to the reference pattern (133), detected in the first digital image and the second digital image, a first part of the code pattern (134) corresponding to the first area (134a) of the code pattern detected on the first digital image and a second part of the code pattern (134) corresponding to the second area (134b) of the code pattern detected on the second digital image, and storing the obtained composite digital image in the memory;

reading and decoding with the processor the code pattern (134) from the stored composite digital image;

wherein the system is further adapted to carry out the steps of:

extracting from decoded data of the code pattern a user identity data and a digital signature of said user identity data, via image processing and decoding operations with the processor, and storing the extracted user identity data and digital signature in the memory;

sending a first message (M1) containing the extracted user identity data and digital signature stored in the memory via the communication unit (CN) to the server (S);

decrypting at the server (S) the extracted digital signature received in the first message (M1) from the portable device (200) with the decryption key stored in the database (DB), and checking whether the extracted user identity data received in the first message (M1) matches the received extracted digital signature; and

in case of matching, sending back to the portable device (200) a server message (SM) indicating a successful verification of the user identity data.

15. The system according to claim 14, wherein

the server (S) is further adapted to send data via the communication network (CN) to a communication device of the user; and

the server (S) and the portable device (200) are further adapted to carry out the steps of the method according to any one of claims 12 and 13 of verifying the security document (150) of the user.