A smart passport comprising a smart inlay that includes a core substrate operative to store and exchange information contactlessly with an external reader, at least one physical security component coupled to the core substrate and operative to render the smart inlay and thereby the passport tamper-proof, and a logical security component incorporated in the core substrate and operative to render the smart inlay and thereby the passport forgery-proof. The physical security component is preferably selected from the group at least one tear line and at least one patterned adhesive, both operative to cause irreversible damage to the information storage and communication capabilities of the passport in case of tampering.
Fig. 1a
Smart Passport Inlay

Fig. 1b
Fig. 1c
Fig. 2
Fig. 4
TAMPER-FREE AND FORGERY-PROOF PASSPORT AND METHODS FOR PROVIDING SAME

FIELD OF THE INVENTION

The present invention relates to tamper-free and forgery-proof identification documents, and in particular to smart passports.

BACKGROUND OF THE INVENTION

Security, particularly at major airports has become a significant concern. No printable identification is currently available to positively identify a passenger with high reliability. No means is currently available to transmit such information securely and to associate that information with user specific permissions.

All passengers entering the USA have been required to bring a Machine Readable Travel Document (MRTD), i.e. a machine-readable passport since October 2003. Starting October 2004, the passport is required to contain biometric data that uniquely identifies its bearer. This turns the passport into a “smart” passport, which comprises a contactless chip that stores the personal biometric information as digital information. The chip is accessed contactlessly by a reader that retrieves the biometric information and compares it with information stored in a database, to verify the identity of the passport bearer. The International Civil Aviation Organization (ICAO) is setting the standard to be followed by all such smart passport issuers.

Smart documents are known in the art. Smart cards have been used to store personal information and even biometric information about their owners to facilitate electronic transactions. The information is stored on embedded chips, see for example U.S. Pat. No. 6,219,439, the content of which is incorporated herein by reference. U.S. Pat. No. 6,219,439 further describes a identifying characteristic authentication system using a smart card having stored physiological data of a user on a chip disposed therein, and a fingerprint scan (or retina scan, voice identification, saliva or other identifying characteristic data) for comparison against the stored data. The system is self-contained so that the comparison of the identifying characteristic data with the data stored on the chip is done immediately on board the reader without relying upon communications to or from an external source in order to authenticate the user. This arrangement also prevents communication with external sources prior to user authentication being confirmed, so as to prevent user data from being stolen or corrupted.

U.S. Pat. No. 6,101,477 describes a smart card for travel-related use, such as for airline, hotel, rental car, and payment-related applications. Memory space and security features within specific applications provide partnering organizations (e.g., airlines, hotel chains, and rental car agencies) the ability to construct custom and secure file structures. U.S. Pat. No. 5,291,560 describes a personal identification system based on iris analysis. U.S. Pat. No. 5,363,453 describes a personal identification system based on biometric fingerprint data. However, there is no encryption of the biometric information involved.

EP 0019191B1 discloses a paper of value (e.g. an ID) with an integrated circuit in which a checkable coding is written, the communication with the integrated circuit preferably being effected contactlessly via antennas. The integrated circuit is set in the gap of an at least partly metalized carrier foil. This foil is then laminated between two paper webs. Since the carrier foil is only laminated between the two paper webs, however, there is the danger that the layers can be separated from each other relatively easily so that the plastic inlay provided with the chip can be used for possible forgeries. Further, this security element is a strictly machine-checkable security element that can only be checked by means of special detectors.

U.S. patent application 20030164611 by Schneider discloses a security paper for producing documents of value, such as bank notes, certificates, etc., with at least one multilayer security element. The security element is disposed at least partly on the surface of the security paper and has at least one visually checkable optical effect and at least one integrated circuit. Other recent U.S. patent applications relevant to the subject of the present invention include applications Nos. 20040018132, 20030117262, 20030116630, 20030093379, 20030093187 and 20020143588.

All prior art solutions deal with only partial aspects of the problem. All known solutions require basically a new product, fabricated with processes and steps materially different from existing processes and steps used in present day regular (non-smart) passports. Since these processes and steps differ from each other, there is no “standardized” manufacturing of a smart passport. No prior art solution is known to be a full solution that allows a regular passport to be transformed into a smart passport without requiring major production system changes and/or major fabrication step changes. Therefore, it would be advantageous to provide a smart passport that will not require major overhaul of existing methods and systems, yet fulfill its total security and forgery/tamper-proof functions. It would be further advantageous to find a “generic” solution that can incorporate various chips and operating systems (OSs) into the smart passport, which can then be issued by all authorized issuers that use such different chips and OSs.

SUMMARY OF THE INVENTION

The present invention discloses a method and system for providing secure, tamper-free and forgery-proof smart documents, in particular smart passports. The present invention further discloses a smart inlay that has inventive physical security components or “features”, and which can be inserted into any standard passport, thereby turning it into a smart passport. The smart inlay of the present invention is functionally flexible in that provides full accommodation of existing and emerging standards in the filed of smart documents, in particular of smart passports. These standards will include requirements for global interoperability, technical reliability, practicality and durability. The emerging standards will most likely require a digital representation of personal biometric information on a contactless chip in the passport booklet or in a visa. The digital representation will include data. The biometric representation may be that of a face and fingerprint or iris. The contactless chip may be made by a variety of manufacturers, according to the ISO 14443 A/B or ISO 15693 standards. The booklet may include the smart inlay in its cover (using a cover substantially
identical with that of existing, non-smart passports) or in a data page. In a visa, the visa sticker will contain the chip and its antenna.

The biometric information is expected to provide a singular match (comparison) of a person to data stored in a database for identity verification. All digital information on the chip will be cryptographically signed to prevent forgery. The planned biometric storage needs include ca. 12 KB (kilo-bytes) for a face, 10 KB for a fingerprint, 30 KB for an iris and 5 KB for text+overhead. At the least, a smart passport will require will need 32 or 64 KBs. The required antenna size is the same as in ID-1 size documents similar to a credit size card. The inlay has to be mechanically reinforced to protect the inlaid chip and antenna. Finally, the smart passport has to be readable by a contactless reader that supports both ISO 14443A and 14443B standards.

The present invention provides a smart inlay that can accommodate a variety of chips, for example a Philips PCF1072 72K EEPROM or a ST Micro Electronics ST19XR34 34K EEPROM. The present invention further provides an upgrade path from a regular (non-smart) paper passport to a smart passport.

According to the present invention, there is provided a smart inlay comprising a core substrate operative to store and exchange information contactlessly with an external reader, the core substrate further conditioned to bind to a passport surface, at least one physical security feature coupled to the core substrate and operative to render the smart inlay tamper-proof, and a logical security feature incorporated in the core substrate and operative to render the smart inlay forgery-proof.

According to the present invention there is provided a smart passport comprising a passport booklet and a smart inlay incorporated in the passport booklet, whereby the smart inlay imparts tamper-proof and forgery-proof properties to the passport.

According to the present invention there is provided a method for tamper-proofing and forgery-proofing a passport, comprising the steps of providing a smart inlay operative to uniquely identify an authorized bearer of the passport, the smart inlay adaptively fitting into the passport, and attaching the smart inlay to the passport.

According to one feature in the method for tamper-proofing and forgery-proofing a passport of the present invention, the step of providing a smart inlay further includes providing an inlay with a core substrate operative to store and exchange information contactlessly with an external reader, the core substrate further conditioned to bind to a passport surface, at least one physical security component coupled to the core substrate and operative to render the inlay tamper-proof; and a logical security component incorporated in the core substrate and operative to render the smart inlay forgery-proof.

According to another feature in the method for tamper-proofing and forgery-proofing a passport of the present invention, the step of attaching the smart inlay to the passport includes attaching the inlay to the inside of a cover of the passport.

According to yet another feature in the method for tamper-proofing and forgery-proofing a passport of the present invention, the step of attaching the smart inlay to the passport includes attaching the inlay to at least one inside page of the passport.

According to the present invention there is provided a method for preventing tampering in a smart passport that includes a contactless chip physically connected to an antenna, comprising the steps of providing at least one physical security component operative to disconnect the chip from the antenna and using the at least one physical component to protect the smart passport form tamper attempts.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is herein described, by way of example only, with reference to the accompanying drawings, wherein:

**FIG. 1** shows a preferred embodiment of a smart inlay according to the present invention: a) cross-section; b) top view; c) top view of three attached smart inlays; and d) view of a smart inlay trimmed from a strip.

**FIG. 2** shows embodiments of a smart passport incorporating the smart inlay according to the present invention: a) attached to a smart passport cover, b) inserted into the inside of a smart passport booklet.

**FIG. 3** shows schematically steps in the manufacturing of the smart inlay: a) main process steps; b) detail of a patterned first adhesive with "voids"; c) various adhesive patterns overlaid with an antenna.

**FIG. 4** shows schematically a summary of a set of logical operations involved in functionalizing the smart passport and rendering it logically forgery-proof.

**FIG. 5** shows a detailed flow-chart of the operations involved in the fabrication and functionalization of both a smart inlay and a smart passport.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention discloses devices and methods for providing secure, tamper-free and forgery-proof smart documents, in particular smart passports. The present invention discloses in particular a smart inlay to be used in a smart passport, and security features that make such a smart passport tamper-proof and forgery-proof. The present invention further provides an upgrade path from a regular (non-smart) paper passport to a smart passport.

**FIG. 1a** shows in cross section a preferred embodiment of a smart inlay 100 according to the present invention. Smart inlay 100 comprises a core substrate (or "core layer") 102 made preferably of synthetic sheets, e.g. from Teslin manufactured by PPG Industries (www.ppg.com) or Artisyn manufactured by Darmic Inc. (www.darmac.com). Each of these materials provides a number of important advantages: each allows a judicious choice and application of tamper-proof adhesives, for example poly-vinyl-acetates (PVAs), thermoplastic adhesives such as ethylene vinyl acetate (EVA) or polyethylene (PE), or the family of thermo-set adhesives. Teslin and Artisyn are further advantageous in that one can use most adhesives or glues that are water-based, solvent-based or heat or pressure activated, single or dual component. Alternatively, the core substrate material
may include Vinyl or Polyurethane based materials. Smart inlay 100 further comprises an embedded contactless chip module 104 that includes an encapsulated chip 106 and a lead frame 108, and tearing lines (“tear lines”) 110 that provide a first main inventive security component. Tear lines 110 are preferably positioned under the lead frame electrodes. Alternatively, in some embodiments, the tear lines may extend the whole width of the inlay, to provide added bending flexibility (in addition to a weak spot) to the passport into which the inlay is incorporated (see below). Smart inlay 100 further comprises an antenna 120 that allows two-way communication between the chip and an outside contactless reader system (not shown). The chip module is electrically connected to the antenna through the lead frame. Optionally, smart inlay 100 further comprises a cover material 112 attached to the core by a thin layer of adhesive 114, preferably a highly solvent resistant adhesive, and more preferably a thermo-set type adhesive with a relatively high bond breaking temperature, e.g. serial number 9534 manufactured by Apollo (www.apolloadhesives.com), 3M (www.3m.com) adhesive sheet 9218, 9200 or 9328, or Scapa Tape G175 (www.scapatapesnacon). The core substrate has a typical thickness of 220-240 micron, while the smart inlay has a typical size that fits in a page of a smart passport, see for example FIG. 1b. Other dimensions in FIG. 1a are marked H1, typically 380 microns, H2, typically 30 microns, H3, typically 350 microns and H4, typically 20-50 microns. Advantageously, the chip may be any standard chip such as a Philips PS5CT072 72K E²PROM or a Thompson ST19XR34 34K E²PROM.

In FIG. 1b shows in a top view a smart passport inlay (“smart cover”) with vinyl cover 120 (normally inserted in the “back cover” of a passport, see below) complemented by a “dumb” section 122 (normally inserted in a “front cover” of a passport, see below), both with typical dimensions indicated on the figure. As shown in FIG. 1c, for efficient production purposes (described in more detail in FIG. 3c), the smart inlay may be included in a set of attached smart inlays on a continuous reel, in this case three inlays 130, 132 and 134. FIG. 1d shows a single smart inlay 150, cut away from the continuous reel. The dimensions shown in both FIGS. 1b and 1c are exemplary only, and in no way limiting.

FIG. 2a shows a smart passport booklet 200 that includes a smart inlay 202 incorporated into a cover 204 (usually a back, fiber-reinforced vinyl cover, for example one manufactured by ICG Holliston (www.icg-holliston.com)). The figure further shows an external booklet page 206 and the rest of the booklet contents 208. FIG. 2b shows a smart passport booklet 200 in which a smart inlay 210 is incorporated between two internal pages 212 and 214. In this case, the inlay may be either glued to one or both of the internal pages, attached directly to the passport backbone, or both. The attachment to the passport backbone can be done either by sowing part of the inlay into the backbone, by lamination to a cover or to a page, by gluing, or by other known means.

FIG. 3a shows schematically steps in a preferred manufacturing process of the smart inlay of the present invention. The manufacturing is performed in a system in which a continuous material strip 300, preferably made of Teslin or Artisyn is fed by a reel. Smart inlay cores with a top surface 301a and a bottom surface 301b are part of strip 300. First, a chip hole 302 and local weakening patterns in the core layer, referred to hereinafter generically as “tear lines” 304 are fabricated (e.g. punched) in the feed strip in a step 350. The tear lines are designed to provide a local weak link in the smart inlay, so that any attempt to separate the core layer from the cover will lead to irreversible core substrate deformation and mechanical destruction of the antenna/chip assembly. That is, such an attempt will cause the separation of the antenna from the chip, or the breakup of the chip electrode/lead frame. This is one main inventive physical feature of the smart inlay of the present invention. The tear lines may be in the form of perforations, preferably positioned under the electrode area as shown in FIG. 1a or as thinned areas in the core layer in the same places. Any attempt to tamper with the finished inlay, e.g. trying to separate the core layer from the vinyl cover (or from an internal cover or page if the inlay is inserted between two booklet pages) will result in the failure described above. A first adhesive pattern 306 designed for antenna positioning and securing to the core (also referred to herein as “antenna base adhesive”) is deposited on top surface 301a in step 352. The antenna base adhesive pattern may be variable in size and shape, and may cover either partially or substantially totally the area of the top surface. In case it covers substantially the entire inlay surface, this may be the only adhesive layer applied in the manufacturing process. The adhesive may be any type of adhesive, for example PE or EVA, an adhesive such as 3M adhesive sheet 9218, 9200 or 9328, Scapa Tape G175, or a pressure sensitive adhesive such as D74 manufactured by Colquimica (www.colquimica.pt).

In the case of the first adhesive layer being the only layer in the process, the preferred adhesive is a thermo-set adhesive such as serial number 9534 manufactured by Apollo (www.apolloadhesives.com). Thermo-set adhesives behave irreversibly and have a wide range of bond-breaking temperatures that reaches over 200 degrees C. This makes the adhesive itself the “strong” link in the composite layer structure, and ensures failure in places other that the adhesive, providing yet another inventive physical security feature. Furthermore, if the first adhesive is the only adhesive used, it is further preferably patterned, as explained with reference to FIG. 3c below. As used herein, a “patterned” adhesive means any non-smooth, irregular adhesive surface, layer thickness, or general appearance. Preferably, the pattern follows some regular periodic form or topology such as regular corrugations, mesh, waves, zigzag, spring-like, or other geometric shapes. Inventively and advantageously, the first adhesive pattern may be segmented or placed in a patterned structure 306 that has gaps or “voids”, as shown in FIG. 3b. This allows a second adhesive (glue) layer 114 (see below) to fill the gaps, creating a composite structure of the two glues and further strengthening the product. In other words, the non-smooth and non-uniform application of the first glue layer that leads to the formation of a composite, interlaced, or intermingled structure with the second adhesive, results in even greater resistance to tampering and forgery. If any attempt is made to separate the smart inlay layers, or to separate the inlay from the cover or page it is attached to, the strong adhesive composite will cause failure in a non-adhesive “weak spot” and result for example in the tearing of the antenna or of the smart inlay layer materials, or in the destruction of the chip. The glue may be also
layered on the chip area, leading to additional weak spots (added to those provided by the tear lines) which may cause potential breakage of the chip if an attempt is made to separate the layers.

[0032] In step 354, a chip module 308 (shown in more detail in FIG. 1a) is pressed in from the top surface into chip hole 302. In step 356, an antenna 310 is wound on top of the patterned adhesive layer and attached (e.g., welded or soldered) to respective chip connections on the chip lead frame. This is followed by pressing the antenna, typically under additional heating into adhesive pattern 306 to form a flat surface.

[0033] As mentioned, when the smart inlay (and its “dumb” section in case of a smart cover) produced in steps 350-356 is about to be attached to a cover, a second adhesive layer 114 (used if the first adhesive layer does not fulfill that function) is introduced between the inlay and the cover and used to fill any voids in glue layer 306. The introduction of this layer is shown in an additional step 358. It has been determined experimentally that attempts to peel off the inlay from the cover show distinct tampering effects when second adhesive layer 114 is also applied in a patterned form (independently of the form, patterning or even presence of a first adhesive layer), as shown in both step 358 and in a cross section in FIG. 3b, which shows a tooth-like adhesive layer 306” or 114” formed on the core substrate. To emphasize, patterning either or both adhesive layers advantageously improves the security aspects of the smart inlay and passport of the present invention. This constitutes yet another inventive physical security feature of the present invention.

[0034] FIG. 3c shows several exemplary embodiments of geometries of patterned adhesives according to the present invention. Embodiments A-E show a first adhesive overlaid with the antenna, and embodiment H shows a cross section of a composite, two-adhesive structure with the antenna in the middle. In more detail, embodiment A shows a zigzag first adhesive pattern 360 overlaid by an antenna 362. Embodiment B shows a series of glue segments 364 overlaid by an antenna 366. Embodiment C shows a “stretched spring” adhesive pattern 368 overlaid by an antenna 370. Embodiment D shows a full adhesive strip 372 overlaid by an antenna 374. Embodiment E shows a dot adhesive pattern 376 overlaid by an antenna 378. In all cases, “overlaid” preferably also means that the antenna is actually sunk into the adhesive, so that is in the same plane as the adhesive. Methods for deposition of patterned adhesives are well known in the art.

[0035] Embodiment H shows in cross section a composite adhesive structure in which a first adhesive 380 and a second adhesive 382 (both having a tooth-like appearance as in FIG. 3b) are interlocked or interlaced, locking in an antenna 384. The first adhesive is deposited such that it has a plurality of holes, “dips” or “valleys” in the vertical direction perpendicular to the core substrate top surface. The antenna is wound and pressed in, preferably under heat, as described in step 356. The second adhesive layer is then applied, filling in the holes, dips or valleys of the first adhesive, and locking the antenna in place in the composite two-adhesive layer. The cross section in H is in essence an enlargement of line 114 with thickness 114 in FIG. 1a for a specific embodiment. Thus, the two adhesives and the antenna are locked between a core substrate 386 and a cover 388.

[0036] The invention thus advantageously provides a number of physical security features, some of which have been mentioned above and some of which will be discussed in more detail now. All physical security features are geared toward providing a tamper-proof product. First, the tear lines mentioned and shown with regard to FIG. 1a provide security by causing destruction of the functional integrity of the smart inlay (e.g., separation of the antenna from the chip or breakage of either the antenna or the chip) in the case of any tampering attempt. Second, the use of preferably thermo-set adhesives implies irreversibility and allows a choice of high enough bond-breaking temperatures. This ensures that any attempt to separate the different layers results in layers deformation or destruction before adhesive bond breaking. Third, the patterning of either of the first or of the second adhesive (or both coexisting together) provides additional tamper-proof security because the adhesive competes locally in strength with the core material.

[0037] FIG. 4 shows schematically a summary of a set of logical operations involved in fabricating a smart passport and making it logically forgery-proof. The set of operations includes 5 phases, each phase including a physical operation performed on a device, and an attendant logical operation occurring in a computer database. In phase 400, the chip functionality is tested, resulting in the storage (registration) of a chip serial number (CSN) and a chip operating system serial number (OSSN) in the computer database. The database allows to establish a unique logical link between the CSN and the OSSN, referred to herein as “logical link 1”. In phase 402, the complete circuit of the smart inlay including the antenna are functionally tested and the results registered in the database. In phase 404 the smart passport is functionally tested, and a passport serial number (PSN) identifying the passport booklet is retrieved from the booklet and registered in the database. This establishes a second logical link between the CSN, OSSN and PSN, referred to herein as “logical link 2”. In phase 406, the passport is issued to a particular person, and personal information, preferably biometric (e.g., photo, iris, fingerprint, etc.) is inserted into both the passport and the database. At this stage, a unique link (also referred to as “logical link 3”) is created between the passport and the person to which it is issued using a combination of some or all of logical links 1 and 2 and the personal information. This may be done for example by creating a unique “key” or “secret” using encryption or encoding well known in the art. The “key” or the “secret” is stored in the database and optionally in the passport (chip) and may be retrieved after accessing its location in the chip memory using an access key. In phase 408, the smart passport is presented at a border control station to identify its carrier. A check is made to restore the unique “key” or “secret” formed by the combination of logical links 1 and 2 and the personal information of the carrier. The result of this check is matched against the stored “key” or “secret” stored in the database and optionally in the passport. If there is no fit, the implication is that the carrier and the passport do not match, and/or that the passport is forged.

[0038] FIG. 5 shows a detailed flow-chart of the operations involved in the fabrication and functionalization of
both a smart inlet and a smart passport. The process starts with the fabrication of the smart inlay substrate, in a system that may be substantially similar to that described for smart cards in U.S. Pat. Nos. 6,108,022 and/or 5,973,710 to Landsman. Following essentially the steps in FIG. 3a, chip holes and weakened substrate areas (tear lines) are made in a core substrate in step 502, followed by spreading of the antenna glue base (first adhesive layer) in step 504, and insertion of the encapsulated chip into the hole in step 506.

At this point, a chip functionality test (process 400 in FIG. 4) is run in step 536 to test Go/NoGo chip functionality and to essentially form logical link 1 as described above. If the test fails, the chip is rejected in step 538 and another chip is placed in the hole. If the test is successful, the antenna is wound on the adhesive layer in step 508, its wires are trimmed (cut) in step 510 and the antenna is welded to the chip electrodes in step 512. The chip and antenna are then levelled flush with the top surface of the core substrate in step 514. A second test (process 402 in FIG. 4) is run to test circuit functionality, i.e. to confirm that the circuit is active.

If the test fails, the smart inlay is marked and trimmed into a strip in step 518 and placed in an exit tray in step 520 (resulting in the product seen in FIG. 1b). To produce a smart cover, a blind inlay substrate material similar to the smart inlay core is supplied in step 522, a preferably vinyl cover material is supplied in parallel in step 524, and all three elements (smart inlay substrate, blind inlay substrate and cover) are bound together in step 526. The binding is preferably done by applying the second adhesive layer to either the inlay, the cover or both. The layers are bound under pressure and heat (depending on the type of glue) in step 528, followed by a third test (process 404 in FIG. 4) in step 530, following which a defected smart cover is marked. A “good” smart inlay is trimmed to strips in step 532 and placed in an exit tray in step 534 (resulting in the product shown in FIG. 1c).

The smart passport is now prepared using the smart inlay provided in step 534. If in the form of a smart cover, the smart inlay is glued or attached otherwise to a passport booklet in step 550, the booklet is folded in step 552, and each individual passport is cut in step 554. A fourth test (process 406 in FIG. 4) is run in step 556. If the test fails (passport does not respond to a reader), the smart passport is marked as rejected and placed in a reject bin in step 560. If the test succeeds, the passport is ready for issuing and placed in an exit tray in step 558.

All publications, patents and patent applications mentioned in this specification are herein incorporated in their entirety by reference into the specification, to the same extent as if each individual publication, patent or patent application was specifically and individually indicated to be incorporated herein by reference. In addition, citation or identification of any reference in this application shall not be construed as an admission that such reference is available as prior art to the present invention.

1. A smart inlay comprising:
   a. a core substrate operative to store and exchange information contactlessly with an external reader, said core substrate further conditioned to bind to a passport surface;
   b. at least one physical security component coupled to said core substrate and operative to render the smart inlay tamper-proof; and
   c. a logical security component incorporated in said core substrate and operative to render the smart inlay forgery-proof.

2. The smart inlay of claim 1, wherein said core substrate includes a contactless chip module for providing said information exchange operativeness and an antenna connected to said chip module for providing said information exchange operability.

3. The smart inlay of claim 1, wherein said at least one physical security component is selected from the group consisting of at least one tear line and at least one patterned adhesive.

4. The smart inlay of claim 3, wherein said at least one patterned adhesive is a thermo-set adhesive.

5. The smart inlay of claim 3, wherein said at least one patterned adhesive includes two patterned adhesives forming a composite adhesive structure.

6. The smart inlay of claim 3, wherein said at least one patterned adhesive includes two patterned adhesives forming a composite adhesive structure.

7. The smart inlay of claim 1, wherein said logical security feature includes a unique key obtained from a combination of a first logical link, a second logical link and personal information.

8. The smart inlay of claim 1, wherein said core substrate is made of a material selected from the group consisting of Teslin and Artisyn.

9. A smart passport comprising:
   a. a passport booklet; and
   b. a smart inlay incorporated in said passport booklet, said smart inlay further including:
      i. a core substrate operative to store and exchange information contactlessly with an external reader, said core substrate further conditioned to bind to a passport surface,
      ii. at least one physical security component coupled to said core substrate and operative to render the smart inlay tamper-proof, and
      iii. a logical security component incorporated in said core substrate and operative to render the smart inlay forgery-proof,

whereby said smart inlay provides tamper-proof and forgery-proof properties to the passport.

10. The smart passport of claim 9, wherein said smart inlay is attached to a passport cover.

11. The smart passport of claim 9, wherein said smart inlay is attached to an internal page of the passport.

12. The smart passport of claim 9, wherein said at least one physical security component is selected from the group consisting of at least one tear line and at least one patterned adhesive.

13. The smart passport of claim 12, wherein said at least one patterned adhesive is a thermo-set adhesive.

14. The smart passport of claim 12, wherein said at least one patterned adhesive includes two patterned adhesives forming a composite adhesive structure.
15. The smart passport of claim 12, wherein said at least one tear line is selected from the group of a local core substrate thinning and a core substrate perforation.

16. The smart passport of claim 9, wherein said logical security feature includes a unique key obtained from a combination of a first logical link, a second logical link and personal information.

17. The smart passport of claim 9, wherein said core substrate is made of a material selected from the group consisting of Teslin and Arisyn.

18. A method for tamper-proofing and forgery-proofing a passport comprising the steps of:
   a. providing a smart inlay operative to uniquely identify an authorized bearer of the passport, said smart inlay adaptively fitting into the passport; and
   b. attaching said smart inlay to said passport.

19. The method of claim 18, wherein said step of providing a smart inlay further includes providing an inlay that includes:
   i. a core substrate operative to store and exchange information contactlessly with an external reader, said core substrate further conditioned to bind to a passport surface,
   ii. at least one physical security component coupled to said core substrate and operative to render said smart inlay tamper-proof, and
   iii. a logical security component incorporated in said core substrate and operative to render said smart inlay forgery-proof.

20. The method of claim 19, wherein said step of attaching said smart inlay to said passport includes attaching said inlay to a cover of said passport.

21. The method of claim 19, wherein said providing of an inlay that includes at least one physical security component includes providing at least one physical security component selected from the group consisting of at least one tear line and at least one patterned adhesive.

22. A method for preventing tampering in a smart passport that includes a contactless chip physically connected to an antenna, comprising the steps of:
   a. providing at least one physical security component operative to disconnect the chip from the antenna; and
   b. using said at least one physical component to protect the smart passport from tamper attempts.

23. The method of claim 22, wherein said step of providing at least one physical security component includes providing a smart inlay having a core substrate holding both the chip and the antenna, said core substrate further including at least one component selected from the group consisting of at least one tear line positioned in proximity to both the chip and the antenna and at least one patterned adhesive that glues the contactless chip to the antenna.

24. The method of claim 22, wherein said providing of a smart inlay with at least one patterned adhesive includes providing at least one thermoset adhesive positioned to hold both the chip and the antenna.

25. The method of claim 22, wherein said providing of a smart inlay with at least one patterned adhesive includes providing two patterned adhesives forming a composite adhesive structure positioned to hold both the chip and the antenna.

26. The method of claim 22, wherein said providing of a smart inlay with at least one tear line includes providing a tear line selected from the group consisting of a local smart inlay core substrate thinning and a smart inlay core substrate perforation.