159159

Andersen Consulting Unternehmensberatung GmbH,
Otto-Vogler-Str. 15, 65843 Sulzbach

G00002

"System and Method for Automatically Controlling the Crossing of a Border"

The present invention relates to a system and a method for automatically controlling the passing of a border.

Border controls, e.g. at airports, but also in the area of land and ferry traffic, are crucial with respect to time for passenger traffic crossing borders. At the same time, the expense of the control authorities has increased overproportionately in the last few years vis-à-vis the number of travellers, among other things, due to the Schengener agreement. The mobility of people that has been increasing for years and the growing number of passengers in international air traffic lead to new requirements in passenger transportation. On the other hand, personal and financial resources of the state control authorities, air transportation companies and airport operators as well as spatial factors are increasingly limited at many international passenger airports.

Thus, the object of the invention is to increase the speed of passenger traffic.

According to the invention, this object is solved by a system for automatically controlling the crossing of a border with:

- a device for the acquisition of personal data of system users,

- a device for the acquisition of biometric data of system users,

- a device for transferring the personal data of the system users to a search data bank and querying whether the respective system user is on a wanted list,

- a device for storing data that includes the personal data and biometric data of the respective system user on an identification medium that is provided for each system user and, opitonally, identification medium specific data when the result of the search query is negative,

- a pass-through gate situated in front of a border for regulating the passage of system users, having an entrance and an exit, said entrance and exit being closed in the normal position,

- a device for separating the system user situated in front of the entrance to the pass-through gate,

- a device for reading the data stored on the identification media arranged behind the separating device but in front of the entrance to the pass-through gate,

- a device for checking the authenticity of the identification media arranged in front of the entrance of the pass-through gate,

- a device for checking the presence of a manipulation of the data on the respective identification medium arranged in front of the entrance of the pass-through gate,

- a device for opening the entrance of the pass-through gate when the authenticity of the respective identification medium has been determined and no manipulation of the data on the respective identification medium has been found,

- a device located in the pass-through gate for acquiring

biometric data of a system user who has been allowed to enter,

- a device for comparing the acquired biometric data with the biometric data stored on the identification medium of the system user who has been allowed to enter,

- a device for triggering an alarm signal when the acquired biometric data and the biometric data stored on the respective identification medium do not agree,

- a device for transferring the personal data to the search data bank and for querying whether the system user is on a wanted list, and

- a device for opening the exit of the pass-through gate and enabling the system user to cross the border when the result of the search query is negative and for triggering an alarm signal if the result of the search query is positive.

Furthermore, the object is solved by a method for automatically controlling the crossing of a border that comprises the following steps:

- acquiring personal data of system users,

- acquiring biometric data of system users,

- transferring the personal data of the system users to a search data bank and querying whether the respective system user is on a wanted list,

- storing data that includes the personal data and biometric data of the respective system user on an identification medium that is provided for each system user and, optionally, identification medium specific data when the

result of the search query is negative,

- separating a system user who is attempting to cross a border in front of a pass-through gate, having an entrance and an exit, said entrance and exit being closed in the normal position,

- reading the data stored on the identification medium,

- checking the authenticity of the respective identification medium,

- checking the presence of a manipulation of the data on the respective identification medium,

- opening the entrance of the pass-through gate when the authenticity of the respective identification medium has been determined and no manipulation of the data on the respective identification medium has been found,

- acquiring biometric data of a system user who has been allowed to enter the pass-through gate,

- comparing the acquired biometric data with the biometric data stored on the identification medium of the system user who has been allowed to enter,

- triggering an alarm signal when the acquired biometric data and the biometric data stored on the respective identification medium do not agree,

- transferring the personal data to the search data bank and querying whether the system user is on a wanted list, and

- opening the exit of the pass-through gate when the result of the search query is negative or triggering an alarm signal

if the result of the search query is positive.

In particular, it can be provided in the system that the device for acquiring personal data of system users has a device for automatically reading the personal data. For example, the device for automatically reading the personal data can be a scanner.

Advantageously, the device for acquiring biometric data comprises a device for the acquisition of a fingerprint and/or the structure of the retina and/or the facial features and/or the voice and/or language of a respective system user.

A further special embodiment of the system is characterized by a device for processing the acquired biometric data and converting it into one or more representative data feature(s), with the aid of which it is possible to recognize the system user at the control.

It can also be provided that the device for storing data has a device for coding the personal and/or identification medium data and for generating an identification medium specific key.

Furthermore, it can also be provided that the coding device is a locally provided security module or is located in a background system that is linked via an on-line data connection.

Preferably, the device for storing the data has a device for electrically personalizing the coded data in the identification medium and/or a device for affixing the personal data and, optionally, a photo as well as the signature of the respective system user to the identification medium. For example, the personal data can be affixed to the identification medium in thermotransfer printing.

Advantageously, the device for storing the data has a device for coating the identification medium with a laminated film. The

identification medium becomes counterfeit-proof due to the laminated film.

Preferably, the identification media are Smart Cards.

Advantageously, at least one video camera is provided in the pass-through gate. This makes it possible to monitor the pass-through gate, in particular with respect to undertaking an effective separation.

It can furthermore be provided that the device for reading the data stored on the identification media has a device for converting the identification medium specific code from the coded identification medium data and verifying it. This enables a card authentication test.

Furthermore, the device for reading the data stored on the identification medium preferably has a device for decoding the coded personal data and verifying same. This enables a personal legitimization test.

A further special embodiment of the invention is characterized by a device for generating and distributing keys for the data coding and monitoring the system operation. A device of this type performs the function of a Trust Center.

A further special embodiment of the invention is characterized by a device for managing and monitoring, in particular, the life cycle of all identification media issued to system users.

Finally, a further special embodiment of the invention is characterized by a device for cryptographically coding data transferred between devices of the system and/or between the system and external devices. This is to protect against unauthorized access to the data transferred.

The subclaims 17 to 26 relate to advantageous further developments of the method according to the invention.

The invention is based on the surprising finding that the handling of border traffic is accelerated and simplified by integrating the official controls in the overall process, wherein a part of the control is in principle preferred, without the quality of the control suffering as a result. Due to the at least partially preferred control, the control at the border can be simplified and shortened with respect to the unproblematic travellers already previously controlled, as a result of which the police and control forces can concentrate on potential perpetrators and dangers.

The previously performed control enables a mechanical check of the border-crossing tourist traffic that is unproblematic for the police with all the individual components that a border control by police officers also includes, namely comparison of people, authentication of border-crossing documents, search query, permission to cross the border. Taking all national, Schengener and EU requirements into account, travellers previously classified as unproblematic by the police, who had applied and voluntarily supplied personal data and biometric data stored on their identification media, are each immediately mechanically identified and checked by the police via an on-line search query.

Further features and advantages of the invention are found in the claims and in the following description in which an embodiment is described in greater detail with reference to the schematic drawings, showing:

Fig. 1 a top view onto a part of a system according to a special embodiment of the present invention, and

Fig. 2 schematically, essential devices and device

blocks of the system.

Fig. 1 shows a top view onto a part of a system according to a special embodiment of the invention. The part shown relates to the control of system users directly at a border (e.g. a national border). Fig. 1 shows a pass-through gate 10 with an entrance 12 and an exit 14. The entrance 12 and the exit 14 are each provided with a revolving door 16 and 18, respectively. A device for separating the system user is located in front of the revolving door 16 at the entrance 12 (not shown). The user can be separated mechanically or also e.g. optically. For example, traffic lights can be used for this purpose. When the traffic light is green, a single person may pass. If a person proceeds on red, an optical and/or acoustical alarm is triggered. A card reading device 20 is located between this device and the revolving door 16 for reading Smart Cards. In the normal position, the revolving door 16 is stopped and thus locks the entrance 12. A biometric data reading device 22 is located in the pass-through gate 10. The card reading device 20 and the biometric data reading device 22 are linked with a local server of the Federal Border Police (not shown). In addition, there is a video camera 24 in the pass-through gate 10 for monitoring the mechanical separation of the system user.

Fig. 2 schematically shows the essential devices individually or in blocks of the system. A system block, which is provided with the reference number 26, relates to the application for and issuance of a card (so-called Enrolment Center). The card in the form of a Smart Card 28 serves as authorization proof for every system user. When crossing a border, it is checked in the part of the system shown in Fig. 1, which is described here as a decentralized automated border control system 30. The decentralized automated border control system 30 comprises a local server of the Federal Border Police that is linked, via a department server 32 of the Federal Border Police, with a search data bank 34 of INPOL, a Trust Center 36, a central data

management device 38 of the Federal Border Police and the Enrolment Center 26.

One can apply for a card in the Enrolment Center 26. It comprises all process steps that are required to acquire the potential system users, i.e. in particular to acquire their personal and biometric data. Several Enrolment Centers can be provided which are set up at various locations. To apply for a card, the potential system users present their border-crossing document from which the operator of a PC, on which the acquisition software is running, automatically or manually records the data. The data record is printed out on a form and signed by the potential system user who has applied for a card. The form contains, among other things, the following additional information:

- a description of the system,

- the personal data of the potential system user,

- the conditions for the voluntary participation in the system,

- the necessary legal declarations regarding the protection of the privacy of personal data for collection, storage, transfer and processing of the personal data of the potential system user making the application in association with the automated border control,

- a reference to the system user's obligation to carry a valid border-crossing document each time said user crosses a border, and

- a reference to the accepted purposes of a trip for which the system can be used.

In a next step, the fingerprint of the potential system user is taken by means of a fingerprint reading device (not shown). The data obtained from the fingerprint reading device is converted into one or more representative data features by the processing software; it then becomes possible to identify the system user at the border control by means of said data features. Duplication is then tested, i.e. it is checked whether the applicant is already in the system. The previously acquired personal data is supplemented with the biometric data and transferred for coding. This takes place either in the local system in a security module provided therefor or in a background system to which an on-line data link is switched for this purpose. The coded data is electrically personalized in the Enrolment Center to form a Smart Card blank and the personal data applied by thermotransfer printing to the body of the Smart Card. In addition, a photo of the system user as well as his personal data (both, if required, as basis for a manual check, e.g. within the scope of spot check controls), his signature and the name of the issuing Enrolment Center can optionally also be printed on said card. The body of the Smart Card is then coated with a counterfeit-proof laminated film. All these steps take place in a machine and are monitored by the PC. After a function control on a terminal in the Enrolment Center, the Smart Card is issued to the system user. The entire enrolment lasts less than 10 minutes. The card application and issuance can also be done on the spot at the same time when first using the system at the border.

An official of the border control authority reserves the right to take all sovereign steps - carrying out the preferential border control in accordance with the national, Schengener and EU requirements and the release of the Smart Card. If required, he is assisted by personnel or authorized agents of the authority. Appropriate access controls are also provided for fellow employees in the Enrolment Center.

Moreover, the acquisition software ensures that Smart Cards are issued only with aid of legitimate border control officials, only after a successful completion of all necessary steps and only for visa-exempt nationals of specific authorized countries who are in possession of a valid travel document.

The card control comprises all methods that are carried out when the card owner is checked during entry. The card control occurs in the pass-through gate 10 (see Fig. 1) which the person to be controlled must enter.

The pass-through gate itself can be integrated into the existing infrastructure without difficulty, that is, only slight structural modifications are required. The local Server is used to control the process and to communicate with external computers.

A mechanical separation by means of a device for the mechanical separation (not shown) first takes place in front of the pass-through gate 10 to prevent entry of unauthorized persons as well as several persons at the same time. This feature is complemented by the use of a video camera 24 in the pass-through gate 10 and corresponding image interpretation software.

Behind the device for separation but before the entrance 12, the person to be checked is requested to insert the Smart Card in a card reading device 20. A security module (not shown) is located in the card reading device 20 for checking the authenticity of the Smart Card and the personal data stored on it. Every authentic Smart Card has a Smart Card specific key which can be converted by the security module in the card reading device 20 and then verified based on specific Smart Card data. In addition, the communication between the Smart Card and the security module in the card reading device 20 is protected with a temporary key which was previously negotiated between the Smart Card and the security module.

The personal data, including biometric data, is then read from the Smart Card and an affixed signature (MAC) is checked for authenticity with aid of the public key in the security module.

If the authenticity of the card is verified and no data manipulation found, the revolving door 16 can be turned, so that the person can go into the pass-through gate. In the pass-through gate 10, the fingerprint of the system user is obtained by means of the biometric data reading device 22 and compared with the biometric data stored on his Smart Card. In addition, extracts are formed from the locally obtained data and compared with the data features stored in the Smart Card.

Due to this two-step checking method at the entrance to the pass-through gate and within it, two things are attained:

- it is ascertained that the person who was allowed to enter on the basis of the Smart Card checked at the pass-through gate is an authorized system user;

- unauthorized persons are refused entry into the pass-through gate; it should here be sufficient to indicate on a screen at the card reading device at the entrance to the pass-through gate that the person should be subjected to the regular border control.

- Improper users or authorized persons incorrectly refused by the system (this cannot be 100% excluded by any technical system) are reliably determined at the latest in the pass-through gate. In this case, after a corresponding automatic triggering of the alarm by the system, it would be necessary for the border control authority or an authorized agent to intervene in order to release the person from the pass-through gate and direct him to a regular border control.

In the next step, the required personal data is transferred via

the local Server of the Federal Border Police for checking at a search data bank of INPOL.

When all the previously described steps are passed through without difficulties, then the exit of the pass-through gate is opened. In the event of a refusal or a faulty reaction of the system, an alarm is triggered and the person continues to be checked by personnel of the Federal Border Police.

The design of the pass-through gate, the type of separation technology used and the release at the exit of the pass-through gate can be determined in dependency on e.g. the ergonomics and the control of large traffic flows.

The Trust Center 36 serves as a central system component for managing all security-relevant aspects of the system, i.e., in particular, to generate and distribute keys and monitor the continuous operation of the system.

The central data management device 38 of the Federal Border Police is used to manage all Smart Cards issued with functions for monitoring the Card Life Cycle. The card management also includes the functions of application processing, i.e. the acquisition of personal data and biometric data.

The special sensitivity of the data of the Smart Cards and the functionality associated therewith require a high degree of protection against:

- falsification of the personal data on the Smart Card
- falsification of the biometric data
- falsification of the connection between biometric data and personal data

- manipulations at a control terminal

- manipulations when acquiriing the personal data or biometric data, and

- attacks on the cryptographic functions in the system.

To comprehensively safeguard these risks, a shell-type security architecture is advisable for safeguarding central information and functions. The object of the architecture is to establish several hurdles that a potential attacker must overcome to manipulate the system.

The personal data together with the biometric data form the core. This data is considered as a unit in the system, i.e. biometric data is one element of the personal data record. A cryptographic test sum is first generated via the personal data record with aid of a Secure Hash method, e.g. the SHA-1 algorithm. This 160 bit long value has the typical properties of a good hash algorithm, i.e. it is essentially collision-free. The result of the algorithm is used as a part of the cryptogram formation since the entire personal data record is too large as input data for the coding. The hash value compresses the contents of the personal data record to a greatly reduced form. In this case, the original data cannot be inferred from the hash value. Changes in the personal data record result, by necessity, in a change in the hash value. The Secure Hash method is not a coding method, i.e. it does not use a code.

In the second shell, essential extracts from the personal data (e.g. name, date of birth and place of birth), i.e. in particular the data for querying the INPOL search data bank, together with the hash value are coded with a Private Key method. RSA with a key length of at least 1.024 bits or elliptical curves with sufficient key length should be used as a Private Key method, dependent on the further detail coordination.

The private key of an issuing office or the private key of a central agency is used to code the extract. In the latter case, the personal data record must be sent to the central agency for coding and only then can it be personalized in the Smart Card (e.g. by an on-line query).

The public key is required for decoding the extract. It is filed in the control terminal. A decoding first delivers the personal data for the INPOL query and the hash value. The hash value is compared with a reconverted hash value. When they are the same, it can be assumed that it is a genuine data record.

Within the method, a series of variations are possible, the use of which depends on the concrete basic requirements:

- A clear Smart Card number could be incorporated in the personal data record and, as a result, be interlinked with it. Thus, it would not be possible to transfer the data to another Smart Card. An appropriate use of this option requires an on-line personalization, in wihch the personal data and the Smart Card number are coded and personalized directly in the Smart Card.

- The personal data record can be coded with the private key of the issuing office. It would then store its public key in the Smart Card. A control station would then use the public key of the issuing office delivered by the Smart Card to verify the extract. To prevent misuse, perhaps the insertion of falsified public keys of an issuing office, the code pairs of the issuing office must be electronically signed by a central agency. A method of this type enables the issuance of the Smart Card without access and authorization by a central system.

Every Smart Card in the system receives a clear serial number when produced. This serial number is the basis of the

cryptographic method that is actively performed by the Smart Card. The Smart Card contains a smart card specific key obtained by deriving the serial number under a master key for authentication.

Authentication takes place implicitly by reading out of the personal data in the so-called PRO mode. The PRO mode is a variation of the read access introduced in ISO 7816 in which the data transferred to the terminal is secured by a Message Authentication Code (MAC). This MAC is dynamically regenerated during each read access to exclude a so-called Replay attack, i.e. the renewed insertion of data that has already been read.

The MAC is generated within the operating system of the Smart Card by using the card-individual authentication key and a random number delivered by the terminal. For this purpose, the terminal contains a security module (e.g. a further Smart Card), a random number generator and the master key which are used to derive the Smart Card key under the Smart Card serial number. The terminal checks, independently and immediately after the data on the Smart Card has been read, the MAC and refuses a card with faulty MAC.

In this connection, it is important that the MAC be generated dynamically by the Smart Card. The key required herefor must be in the Smart Card. A manipulation of the Smart Card, e.g. by duplication, requires access to this card key, which is only possible at high financial expense.

There is also a variation for this protective step, however, it requires a more efficient Smart Card. The asymmetrical method of the elliptic curves can be used instead of a symmetrical method for the MAC formation (usually, triple DES). In this method, the private, card-individual key is stored in the card so as to be protected against read-out and the public key is made readable. In addition, the public key must be signed with the private key of the system operator. A control terminal now only

has to store the less security-critical public key of the system operator and check the authenticity of the card-individual public key with it.

The data is read out in a manner similar to the symmetrical method, with the exception that the MAC is generated by the asymmetrical algorithm.

Methods of this type that are based on asymmetrical cryptography can only be used to a limited extent in Smart Cards due to their high requirements for computational performance. Specifically, the response time behaviour of a solution of this type must also be taken into consideration here.

The transfer of data between devices of the system, in particular the transfer of data when issuing cards, should be secured by cryptographic methods. For this purpose, there are methods of line coding with which protected, transparent data channels can be built up.

The integrity of the data and the confidentiality can be ensured with these methods. The latter is especially significant when generating and distributing the system key.

Embedding the technical systems in a reliable sequence organization (5th shell) is an essential, often underestimated mechanism for securing information systems. The best and longest key methods of the world are of no use at all if the keys are easily accessible. In this case, technical methods can only produce a limited protection, they are often exposed without protection to an attack from within.

A further feature of the 5th shell is the intention to place all security-relevant system devices into the care of the Border Control Authority. From the point of view of the authority, this should ensure that it is not possible to access these system

devices without their assistance and under no circumstances. To this end, not all system devices actually have to be located in the premises of the authorities. The technical operation could also be carried out at an authorized agent of the authority as long as unauthorized access by third parties (including the operator) is impossible by appropriate contractual assurance clauses.

An additional organisational protective precaution is that all sovereign steps, i.e. performing all the preferential border controls according to the national, Schengener and EU requirements and the release of the Smart Card, are reserved for an official of the border control authority. There are appropriate access controls for him and for the other employees in the Enrolment Center.

In addition, the acquisition software ensures that Smart Cards are issued

- only on the basis of known Smart Card blanks already in the system (every Smart Card blank has a clear card number),
- only with the assistance in the system of legitimate border control officers,
- only after successfully completing all necessary steps, and
- only for nationals of specific authorized countries who are in possession of a valid travel document.

The systems according to the invention have some advantages that differentiate them from various other, to-date unsuccessful, attempts to introduce automated border controls that cover the area:

- The system represents an effective and economical

possibility for making the border control authority more efficient. The system enables border control personnel to focus on a more police-relevant group of persons. As a result, they can provide more for security and service at a lower cost.

- The Smart Card used according to a special embodiment of the invention enables the storage of sensitive data without the risk of misuse due to unauthorized changes or falsifications.

- The method enables the shortest possible transaction times (essentially, only dependent on the response time behaviour of the query of the INPOL search data bank).

- The method enables the lowest possible transaction costs.

- The method does not conceal any problems regarding the protection of personal data (the owner carries his personal data, which is securely protected against unauthorized access, with him.

- The Smart Card used in a special embodiment of the invention contains sufficient storage capacity for this and, optionally, for additional future applications with additional useful potentials.

- There is sufficient space on the Smart Card used according to a special embodiment of the invention to simultaneously optionally use further security features (e.g. machine-readable hologram with microscript) or other storage variations.

The features of the invention disclosed in the preceding description, in the drawings and in the claims can be significant for implementing the invention in its various embodiments, both

individually and in any combination desired.

Andersen Consulting Unternehmensberatung GmbH,
Otto-Vogler-Str. 15, 65843 Sulzbach

"System and Method for Automatically Controlling the Crossing of a Border"

Claims

1. A system for automatically controlling the crossing of a border, having:

- a device for the acquisition of personal data of system users,

- a device for the acquisition of biometric data of system users,

- a device for transferring the personal data of the system users to a search data bank (34) and querying whether the respective system user is on a wanted list,

- a device for storing data that includes the personal data and biometric data of the respective system user on an identification medium that is provided for each system user and, optionally, identification medium specific data when the result of the search query is negative,

- a pass-through gate (10) situated in front of a border (8) for regulating the passage of the system user, having an entrance (12) and an exit (14), said entrance (12) and exit (14) being closed in the normal position,

- a device for separating the system user situated in front of the entrance (12) to the pass-through gate (10),

- a device for reading the data stored on the identification media arranged behind the separating device but in front of the entrance (12) to the pass-through gate (10),

- a device for checking the authenticity of the identification media arranged in front of the entrance (12) of the pass-through gate (10),

- a device for checking the presence of a manipulation of the data on the respective identification medium arranged in front of the entrance (12) of the pass-through gate (10),

- a device for opening the entrance (12) of the pass-through gate (10) when the authenticity of the respective identification medium has been determined and no manipulation of the data on the respective identification medium has been found,

- a device located in the pass-through gate (10) for acquiring biometric data of a system user who has been allowed to enter,

- a device for comparing the acquired biometric data with the biometric data stored on the identification medium of the system user who has been allowed to enter,

- a device for triggering an alarm signal when the acquired biometric data and the biometric data stored on the respective identification medium do not agree,

- a device for transferring the personal data to the search data bank (34) and for querying whether the system user is on a wanted list, and

- a device for opening the exit of the pass-through gate (10) and enabling the system user to cross the border when the result of the search query is negative and for triggering an alarm signal if the result of the search query is positive.

2. System according to claim 1, characterized therein that the device for the acquisition of personal data of system users has a device for automatically reading the personal data.

3. System according to claim 1 or 2, characterized therein that the device for the acquisition of biometric data has a device for the acquisition of a fingerprint and/or the structure of the retina and/or the facial features and/or the voice and/or language of a respective system user.

4. System according to one of the claims 1 to 3, characterized by a device for processing the acquired biometric data and converting it into one or more representative data feature(s), with reference to which it is possible for the control to recognize the system user.

5. System according to one of the preceding claims, characterized therein that the device for storing data has a device for coding the personal and/or identification medium data and for generating an identification medium specific key.

6. System according to claim 5, characterized therein that the coding device is a locally provided security module or is located in a background system which is linked via an on-line data connection.

7. System according to claim 5 or 6, characterized therein that the device for storing the data has a device for electrically personalizing the coded data in the

identification medium and/or a device for affixing the personal data and, optionally, a photo as well as the signature of the respective system user to the identification medium.

8. System according to claim 7, characterized therein that the device for storing the data has a device for coating the identification medium with a laminated film.

9. System according to one of the preceding claims, characterized therein that the identification media are Smart Cards (28).

10. System according to one of the preceding claims, characterized therein that at least one video camera (24) is provided in the pass-through gate (10).

11. System according to one of the preceding claims, characterized therein that the device for reading the data stored on the identification media has a device for determining the identification medium specific key from the coded identification medium data and verifying same.

12. System according to one of the preceding claims, characterized therein that the device for reading the data stored on the identification medium has a device for decoding the coded personal data and verifying same.

13. System according to one of the preceding claims, characterized by a device for generating and distributing keys for the data codings and monitoring the system operation.

14. System according to one of the preceding claims, characterized by a device for managing and monitoring especially the life cycle of all identification media

issued to system users.

15. System according to one of the preceding claims, characterized by a device for cryptographically coding data transferred between devices of the system and/or between the system and external devices.

16. Method for automatically controlling the crossing of a border that comprises the following steps:

- acquiring personal data of system users,

- acquiring biometric data of system users,

- transferring the personal data of the system users to a search data bank and querying whether the respective system user is on a wanted list,

- storing data that includes the personal data and biometric data of the respective system user on an identification medium that is provided for each system user and, opitonally, identification medium specific data when the result of the search query is negative,

- separating a system user who is undertaking to cross a border in front of a pass-through gate, having an entrance and an exit, said entrance and exit being closed in the normal position,

- reading the data stored on the identification medium,

- checking the authenticity of the respective identification medium,

- checking the presence of a manipulation of the data on the respective identification medium,

- opening the entrance of the pass-through gate when the authenticity of the respective identification medium has been determined and no manipulation of the data on the respective identification medium has been found,

- acquiring biometric data of a system user who has been allowed to enter the pass-through gate,

- comparing the acquired biometric data with the biometric data stored on the identification medium of the system user who has been allowed to enter,

- triggering an alarm signal when the acquired biometric data and the biometric data stored on the respective identification medium do not agree,

- transferring the personal data to the search data bank and querying whether the system user is on a wanted list, and

- opening the exit of the pass-through gate when the result of the search query is negative or triggering an alarm signal if the result of the search query is positive.

17. Method according to claim 16, characterized therein that the personal data of the system user is acquired by automatic reading.

18. Method according to claim 16 or 17, characterized therein that the fingerprint and/or the structure of the retina and/or the facial features and/or the voice and/or the language of a respective system user is/are acquired.

19. Method according to one of the claims 16 to 18, characterized therein that the acquired biometric data is processed and converted into one or more representative data feature(s), with reference to which it is possible for

the control to recognize the system user.

20. Method according to one of the claims 16 to 19, characterized therein that the personal and/or identification medium data is coded and an identification medium specific key is generated.

21. Method according to one of the claims 16 to 20, characterized therein that the coded data is electrically personalized in the identification medium and/or the personal data and, optionally, a photo as well as signatures of the respective system user are affixed to the identification medium.

22. Method according to one of the claims 16 to 21, characterized therein that the identification media are coated with a laminated film.

23. Method according to one of the claims 16 to 22, characterized therein that Smart Cards are used as identification medium.

24. Method according to one of the claims 16 to 23, characterized therein that the pass-through gate is monitored by a video camera.

25. Method according to one of the claims 16 to 24, characterized therein that an identification medium specific key is determined from the coded identification medium data and verified.

26. Method according to one of the claims 16 to 25, characterized therein that the coded personal data is decoded and verified.