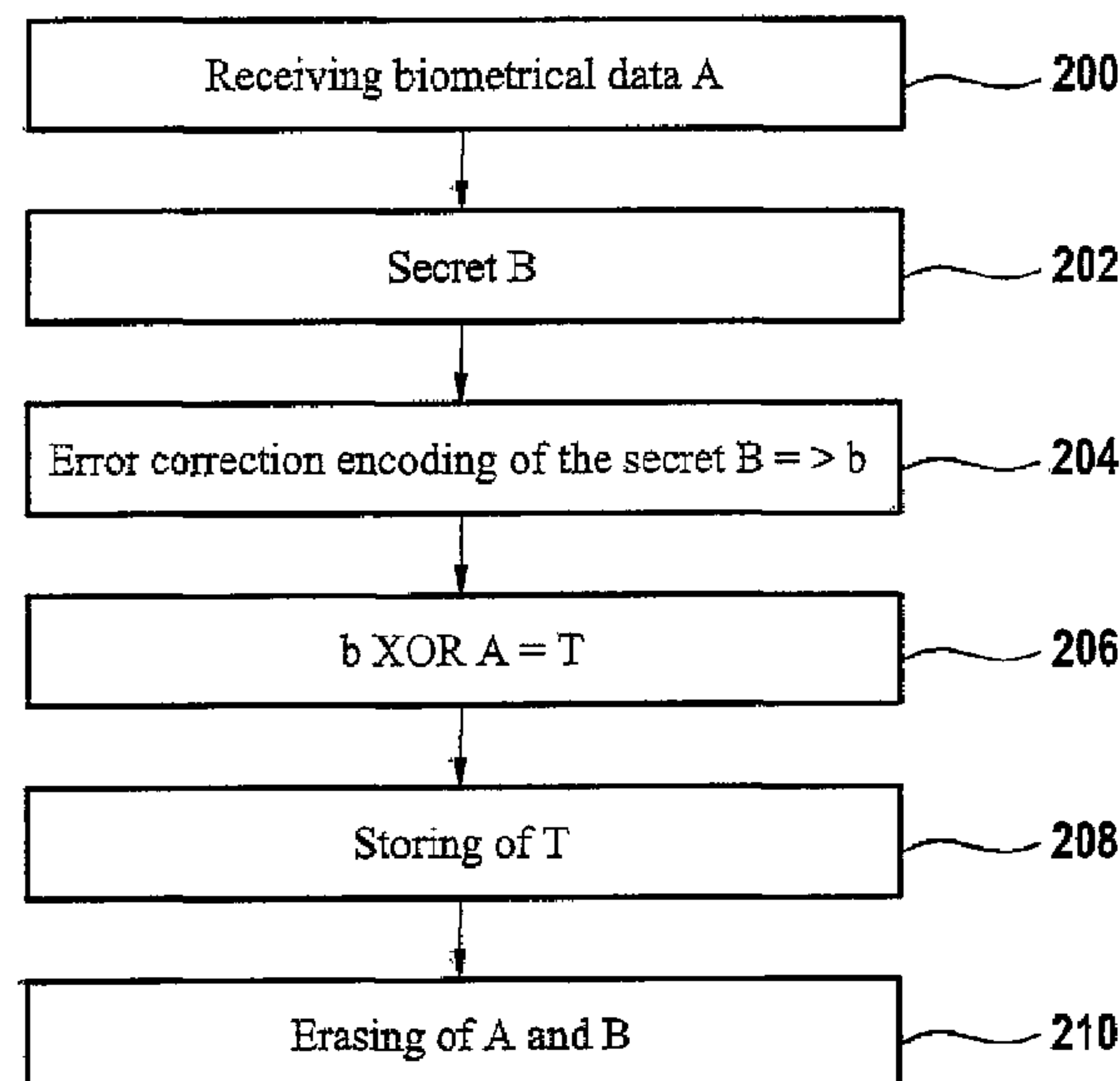




(86) **Date de dépôt PCT/PCT Filing Date:** 2010/11/08
(87) **Date publication PCT/PCT Publication Date:** 2011/05/19
(45) **Date de délivrance/Issue Date:** 2015/08/11
(85) **Entrée phase nationale/National Entry:** 2012/05/11
(86) **N° demande PCT/PCT Application No.:** EP 2010/067002
(87) **N° publication PCT/PCT Publication No.:** 2011/057983
(30) **Priorité/Priority:** 2009/11/12 (EP09175755.9)

(51) **Cl.Int./Int.Cl. H04L 9/32** (2006.01)
(72) **Inventeur/Inventor:**
HUEBNER, THOMAS, DE
(73) **Propriétaire/Owner:**
MORPHO CARDS GMBH, DE
(74) **Agent:** RIDOUT & MAYBEE LLP

(54) **Titre : PROCEDE D'ATTRIBUTION D'UN SECRET A UN JETON DE SECURITE, PROCEDE D'EXPLOITATION D'UN JETON DE SECURITE, SUPPORT DE STOCKAGE ET JETON DE SECURITE**
(54) **Title: A METHOD OF ASSIGNING A SECRET TO A SECURITY TOKEN, A METHOD OF OPERATING A SECURITY TOKEN, STORAGE MEDIUM AND SECURITY TOKEN**



(57) **Abrégé/Abstract:**

A method of assigning a secret to a security token (100) comprising: - receiving first biometrical data (108) of a biomedical feature of a person by the security token, - storing the first biometrical data in the security token, - storing the unencrypted secret in the security token, - biometrically encrypting the secret using the first biometrical data by the security token, - storing the encrypted secret in the security token, - erasing the unencrypted secret and the first biometrical data from the security token.



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
19 May 2011 (19.05.2011)

PCT

(10) International Publication Number
WO 2011/057983 A1(51) International Patent Classification:
H04L 9/32 (2006.01)(21) International Application Number:
PCT/EP2010/067002(22) International Filing Date:
8 November 2010 (08.11.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09175755.9 12 November 2009 (12.11.2009) EP(71) Applicant (for all designated States except US): **SAGEM ORGA GMBH** [DE/DE]; Riemkestraße 160, 33106 Paderborn (DE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **HÜBNER, Thomas** [DE/DE]; Jentzschstraße 3, 33100 Paderborn (DE).(74) Agent: **RICHARDT, Markus**; Richardt Patentanwälte, Wilhelmstraße 7, 65185 Wiesbaden (DE).

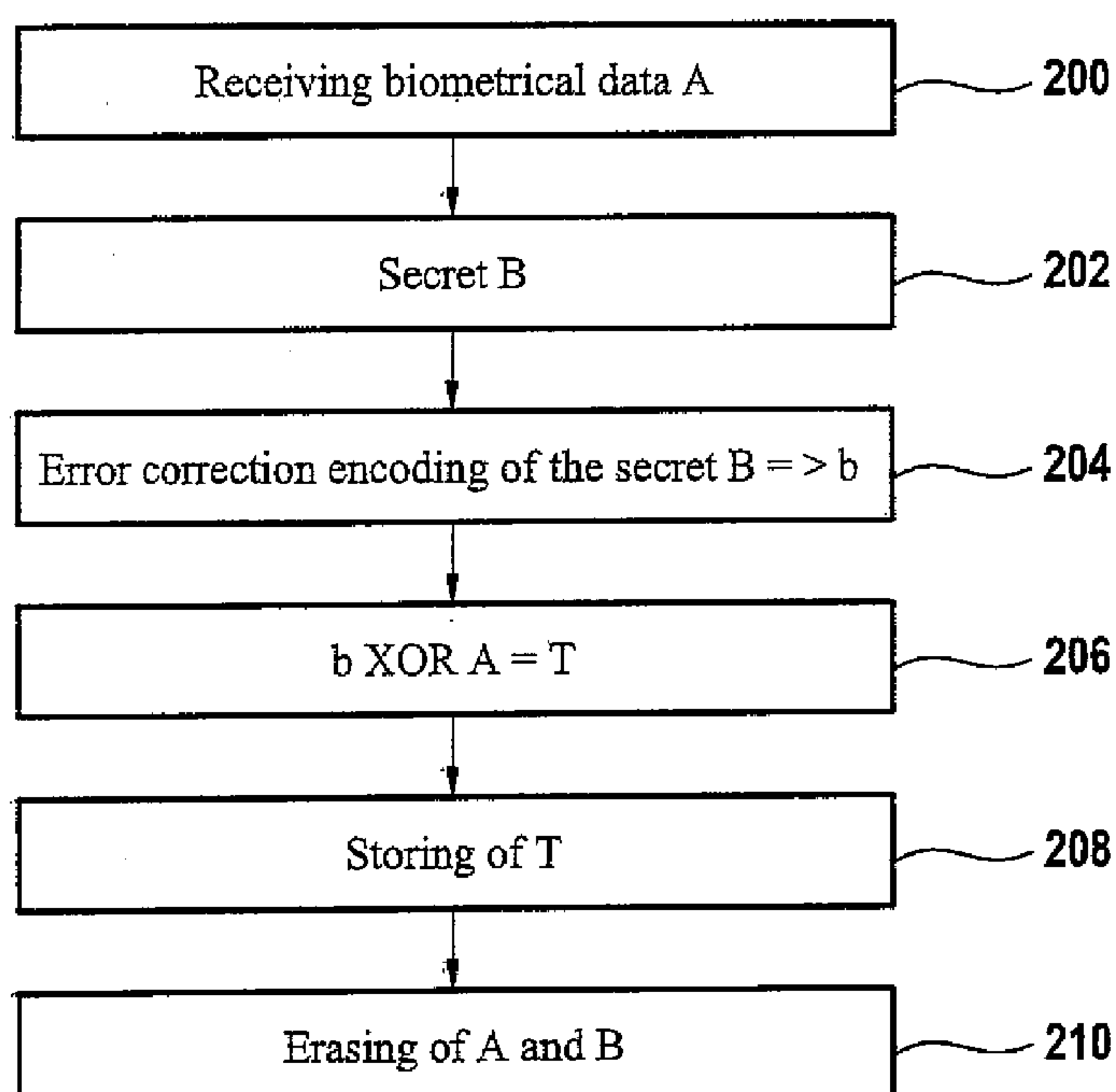
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: A METHOD OF ASSIGNING A SECRET TO A SECURITY TOKEN, A METHOD OF OPERATING A SECURITY TOKEN, STORAGE MEDIUM AND SECURITY TOKEN



(57) Abstract: A method of assigning a secret to a security token (100) comprising: - receiving first biometrical data (108) of a biomedical feature of a person by the security token, - storing the first biometrical data in the security token, - storing the unencrypted secret in the security token, - biometrically encrypting the secret using the first biometrical data by the security token, - storing the encrypted secret in the security token, - erasing the unencrypted secret and the first biometrical data from the security token.

Fig. 3

A method of assigning a secret to a security token, a method of operating a
security token, storage medium and security token

Description

Field of the invention

The present invention relates to the field of security tokens, and more particularly to
5 securely assigning a secret to a security token.

Background and related art

Security tokens are as such known from the prior art. Typically a secret personal
10 identification number (PIN) is stored in a security token for a user's authentication

vis-à-vis the security token. For the purpose of authentication the user has to enter the PIN into the security token which determines whether the stored PIN and the entered PIN are matching.

- 5 Further, security tokens for generating a digital signature are known. A security tokens for generating a digital signature stores a private key of a cryptographic key pair of a user. The secrecy of the private key stored in the security token can be preserved by hardware measures such that when the hardware token is opened, the memory that stores the private key is unavoidably destroyed.

10

WO 00/36566 A1 relates to a biometric identification mechanism that preserves the integrity of the biometric information. A user's private key is stored in a token in encrypted form. The encryption of the user's private key is based upon a biometric encryption key corresponding to the authorized user.

15

WO 2009/009788 A1 relates to an identity authentication and secured access system, component and method. At least one credential issued to one of the users is used, wherein the credential includes a security token comprising data encrypted by encryption software with a cryptographic algorithm and encrypted based on a biometric key that is generated from a biometric identifier of the user.

20

WO 03/100730 A1 relates to a method for generating secure information using biometric information, wherein the method comprises the steps of receiving scan data relating to a person securing data, generating a random cryptographic key, performing a reversible operation on the biometric scan data and said random key to create a template and storing the template.

25

US 7,526,653 B2 relates to a method wherein a private or secret key is encrypted with data obtained from a biometric feature of the owner of the private key. The encryption achieves a guarantee to the effect that the person who has given his digital signature with the aid of the signature key is in fact the rightful owner.

30

WO 2008/010773 relates to a method for generating a cryptographic key from biometric data, wherein the method comprises the steps of acquiring a subject's

PCT/EP2010/0067002

SAGE.209.02 WO

biometric image and extracting characteristic features there from in the form of vector sets, wherein the method further comprises randomly generating a key and applying a mathematical transformation to selected vector sets to encrypt said key, including using a threshold scheme and polynomial functions in a mixture with

5 randomly generated fake vector sets to produce randomly permuted set of elements of the key. Then, a union of the vector sets of the new and fake biometric data with randomly permuted set elements of the key is constructed, which then forms a locked template from the union of values.

10 US 2008/013804 A1 relates to a method and apparatus for authenticating a fingerprint by hiding minutiae, securely storing information on the fingerprint and authenticating the information on the fingerprint in order to prevent the information on the fingerprint from being reused by an attacker who accesses the information of the fingerprint that is stored in a storage unit.

15

US 2002/124176 A1 discloses a biometric identification mechanism in which a token is used for reading biometric data and generating a biometric key. A decrypted private key is used to encrypt a challenge which is used for authentication.

20 WO 2004/05575 A1 relates to key synchronization in a visual cryptographic system. It discloses that hash values can be used to identify a key without compromising it.

Directly using biometric features for encrypting data is highly problematic since fingerprints of an individual are unique to that individual and cannot be changed in

25 case for example the individual's fingerprints are compromised by an unauthorized person. Additionally introducing a user's private key which may be changed as often as required and which is encrypted each time with the biometric encryption data provided by the user permits to provide data encryption and decryption capabilities at a sufficiently high level.

30

However, this security level can only be assured in case the security token used to provide data encryption and decryption capabilities is not lost or stolen. By for

example stealing the security token and using common possibilities to obtain information on the user's fingerprints, it is easily possible to misuse the security token by entering said fingerprints to the security token and perform unauthorized data encryption and decryption processes.

5

The invention aims to provide an improved method of assigning a secret to a security token, a method of operating a security token for performing a cryptographic operation, a storage medium and a security token.

10 **Summary of the invention**

The present invention provides a method of operating a security token for performing a cryptographic operation. The security token has assigned thereto a biometrically encrypted secret. The method of operating the security token
15 includes receiving a second biometrical data of a biometrical feature of a person and a pseudo identity by the security token. The second biometrical data is stored in the security token. The biometrically encrypted secret is read from a memory of the security token. The biometrically encrypted secret is then biometrically decrypted using the second biometrical data by the security token
20 so that the biometrically encrypted secret becomes a biometrically decrypted secret. The pseudo identity is then compared with a hash value of the biometrically decrypted secret. The biometrically decrypted secret is then used to perform the cryptographic operation in case the pseudo identity is identical with the hash value of the biometrically decrypted secret. The biometrically
25 decrypted secret and the second biometrically data is then erased.

A storage medium also is provided. The storage medium is readable by a processor of a security token and contains instructions that when executed by the processor of the security token causes the security token to perform a
30 method in accordance with the previous paragraph.

4a

A security token also is provided. The security token includes means for acquiring biometrical data of a biometrical feature of a person. The token also includes means for receiving the biometrical data in a pseudo identity by the
5 security token. The token also includes volatile storage means for storing the biometrical data in the security token and non-volatile storage means for storing the biometrically encrypted secret. Also included within the token are means for reading the biometrically encrypted secret from the non-volatile storage means. Also included within the token are means for biometrically decrypting
10 the secret using second biometrical data by the security token and means for generating a hash value of the secret. Also included within the token are means for comparing the pseudo identity with the hash values and means for performing a cryptographic operation by using the secret in case the pseudo identity is identical with the hash value of the secret. Also included within the
15 token are means for erasing the decrypted secret and the biometrical data from the volatile storage means.

In accordance with embodiments of the invention there is provided a method of assigning a secret to a security token comprising receiving first biometrical data
20 of a biometrical feature of a person by the security token, storing the first biometrical data in the security token, storing the unencrypted secret in the security token, biometrically encrypting the secret using the first biometrical data by the security token, storing the encrypted secret in the security token, and erasing the unencrypted secret and the first biometrical data from the
25 security token.

A 'security token' as understood herein encompasses any portable physical device that includes a cryptographic function, such as for the purposes of authentication, verification, encryption, decryption or generating a digital
30 signature. Such physical devices include hardware tokens, authentication tokens, USB tokens, in particular USB sticks, chip cards, integrated circuit cards, smart cards, subscriber identity module (SIM) cards, in particular USIM cards, identity documents having an integrated electronic circuit, and RFID tags.

4b

The term 'biometrical data' as used herein may refer to the data delivered by a biometrical sensor, such as a fingerprint sensor or an optical sensor, as a result of biometrical data acquisition, or to the result of processing of biometrical raw data that is delivered by such a biometrical sensor. For example the processing performed by the security token using the biometrical raw data may encompass rounding and/or a projection of the biometrical raw data onto a predefined finite body.

- 10 The term 'biometric encryption' as used herein encompasses any encryption method that uses biometrical data or data that is derived from biometrical data as input information for a given encryption algorithm. For example, the biometrical data

may be used as a key for performing the encryption of the secret or a key is derived from the biometrical data which is then used by the encryption algorithm to encrypt the secret.

5 In accordance with embodiments of the invention the biometrical data is fingerprint data, iris scan data, voice data, or facial biometrical data. The biometrical data can be acquired by means of an external sensor, such as a fingerprint sensor or a camera, that is directly or indirectly coupled to the security token or by a sensor that is integrated into the security token.

10

The secret to be assigned to the security token can be generated by the security token itself, such as by means of a random number generator, or it can be externally selected, such as by a user, and entered into the security token via a communication interface of the security token.

15

Embodiments of the present invention are particularly advantageous as the unencrypted secret is not permanently stored in the security token or elsewhere. After encryption the unencrypted secret is erased as well as the first biometrical data that was used for performing the biometrical encryption operation. As a result
20 only the biometrically encrypted secret is stored in non-volatile memory of the security token. The only way to decrypt the secret is to acquire biometrical data of the same biometrical feature of the same person that was used for the encryption providing an utmost degree of security as regards protection of the secret.

25 Further, in accordance with the invention a hash value of the unencrypted secret is generated by the security token and output for use as a so called pseudo identity (PI) by the person. The PI can be used for authentication purposes vis-à-vis the security token. In other words, the PI can be used as an additional security measure to enable a functionality of the security token.

30

In a practical example, the generation of the hash value may be designed in such a manner that the resulting PI is for example a combination of four digital numbers like '1234'. Thus, these digital numbers can be used in a well known manner as a PIN to authenticate access to security functions of the token. In other words, usage of the

security token requires both, the provision of biometric data, as well as the user PIN, wherein usage of the cryptographic functions of the security token is only enabled in case a user is able to provide both, namely the biometric data and the hash value of the unencrypted secret, i.e. the PIN.

5

The present invention enables a user to arbitrarily change the secret of the security token, wherein with every new change of the secret it is ensured that the personal identifier required to use the security token is also changed. Thus, the security of a respective security token is drastically enhanced. Even though the security token may be lost or stolen and even in case the user's biometric data is publically available, an unauthorized person is still unable to use the token since the person does not know the PI.

10

In accordance with an embodiment of the invention, the security token has volatile storage, such as the random access memory of its processor, and non-volatile memory. The first biometrical data and the secret are temporarily stored in the volatile storage and the encrypted secret is stored in the non-volatile storage. Assuming that the security token does not have an integrated power supply as is typically the case for smart cards, removing the security token from some external device that provides the power supply, such as a chip card reader, automatically erases the biometrical data and the unencrypted secret stored in the volatile storage means.

15

20

In accordance with an embodiment of the invention the first biometrical data and/or the secret are securely erased from the volatile memory while the power supply is still available. This can be implemented by execution of a program module that executes a respective routine for securely erasing the first biometrical data and/or the secret from a RAM of the security token.

25

In accordance with an embodiment of the invention the biometrical encryption of the secret comprises correction encoding of the unencrypted secret.

30

The term 'error correction encoding' as understood herein encompasses any encoding of the secret that allows error detection and correction, in particular by adding

redundant data to the secret, such as by forward error correction (FEC) using convolutional or block codes.

An XOR operation is performed on the error correction encoded secret and the
 5 first biometrical data to provide the biometrically encrypted secret. The biometrically encrypted secret is stored in non-volatile memory of the security token for later use in a cryptographic operation, such as for the purposes of authentication of a user or performing another cryptographic operation, in particular an encoding or decoding operation or the generation of a digital
 10 signature.

For decrypting the biometrically encrypted secret second biometrical data is acquired of the same biometrical feature of the same person from which the first biometrical data was acquired. The second biometrical data typically is not
 15 identical to the first biometrical data due to inaccuracies of the acquisition process of the biometrical data, such as due to inaccuracies of the biometrical sensor that is used for the acquisition, inaccuracies regarding the positioning of the biometrical feature relative to the sensor and/or rounding errors of the algorithm that is used to transform the biometrical raw data delivered by the
 20 biometrical sensor into the biometrical data. Due to the error correction encoding of the secret the correct secret can be recovered from the biometrically encrypted secret even if the second biometrical data is not exactly the same as the first biometrical data. If the second biometrical data is not identical to the first biometrical data as it is typically the case, the result of the
 25 XOR operation performed on the biometrically encrypted secret and the second biometrical data provides a codeword that contains errors. By error correction decoding of the codeword the correct secret is still recovered.

In accordance with an embodiment of the invention a polynomial p is used for
 30 biometrically encoding the secret, such as

$$p(x) = b_0 + b_1x + b_2 x^2 + b_3 x^3 + \dots + b_{k-1} x^{k-1}$$

For encrypting a secret having a number k of digits the polynomial p having degree $k - 1$ is used as the coefficients of the polynomial p are determined by the digits of the secret to be encoded, i.e. the secret being $(b_0, b_1, \dots, b_{k-1})$.

- 5 The first biometrical data is interpreted to be the x -coordinates of points that are located on the polynomial p that is determined by the secret, such as first biometrical data $A = (x_1, x_2, \dots, x_t)$, where t is the number of values contained in the feature set A that constitutes the first biometrical data. Preferably t is greater than k for adding redundancy.

10

Using the x -coordinates provided by the feature set A the number of t points that are located on the polynomial p are calculated. These points on the polynomial p that are determined by the x -coordinates given by the feature set A are referred to as 'real points' in the following, i.e. $P_1 = (x_1, p(x_1))$, $P_2 = (x_2, p(x_2))$, ..., $P_t = (x_t, p(x_t))$.

15

- The number of randomly selected points that are not located on the polynomial p is combined with the real points. These randomly selected points that are not located on the polynomial p are referred to as 'stray points' in the following. For obtaining a total number of r points a number of $r - t$ stray points is added to the set of real points. The set union, which is the union of the set of real points and the set of stray points, constitutes the biometrically encrypted secret wherein no information is stored whether a given point is a real point or a stray point in order to 'disguise' the presence of the real points within the set union.
- 25 Hence, the real points cannot be identified in the set union of the r points by a third party attack. The r points are stored in non-volatile memory of the security token for later use.

- In accordance with an embodiment of the invention the set union is provided in the form of an unordered list that contains data being indicative of the real points and the stray points such as in random order.

30

For decryption of the biometrically encrypted secret that is represented by the set union, the second biometrical data is acquired. The second biometrical data is used to identify at least a subset of the real points within the set union. For example, if an x coordinate given by a value the feature set A' of the second
5 biometrical data matches an x coordinate of one of the r points of the set union that point is considered to be a real point. It is important to note that not all of the real points contained in the set of r points need to be identified this way due to the redundancy that has been added in the encoding operation. Hence, the second biometrical data does not need to be exactly identical to the first
10 biometrical data for obtaining a correctly decoded secret.

From the t values contained in the feature set A' only k values need to match one of the x-coordinates of the r points for identification of k real points. As the k real points unequivocally determine the polynomial p , the coefficients $b_0, b_1,$
15 $\dots, b_{k-1}$ of the polynomial p can be obtained by calculation, such as by resolution of an equation system given by the identified real points. Using Reed Solomon decoding the correct polynomial p can even be recovered if some stray points in addition to the real points are erroneously selected from the set of r points using the x-coordinates provided by the feature set A' .

20

In accordance with an embodiment of the invention the encrypted secret can be stored in a template.

Embodiments of the invention are particularly advantageous as the encrypted
25 secret can be generated by the security token itself, such as by so called on-card generation, without a need to enter the secret. For example, the secret is provided by a random number generator of the security token. This has the advantage that no external storage of the secret needs to occur and no transmission of the secret from an external entity, such as a personal computer
30 or a chip card reader, to the security token that would imply the risk of eavesdropping on the transmission of the secret. Furthermore, embodiments of the invention are advantageous as the personal computer or a chip card reader does not need to be a trusted entity which is due to the fact that no critical data

9a

needs to be communicated from the security token to such an external entity. Moreover, no critical data will be even temporarily generated outside the token (e.g. in the card reader, terminal or PC).

- 5 Alternatively, the biometrically encrypted secret can be generated by an external computer system using the first biometrical data. The biometrically encrypted secret is stored in the security token such as by using a personalization technique. As a further alternative the biometrically encrypted secret is outputted by the security to-

ken via an external interface, such as for use a one-time password or as a cryptographic key.

Embodiments of the invention are particularly advantageous because the encrypted
5 secret does not need to be output by the security token for performing a cryptographic operation such as for the purpose of verification/authentication, decryption, encryption or the generation of a digital signature. Both the decryption of the secret and the performance of the cryptographic operation can be performed by the security token itself such that no sensitive data needs to be output from the security token
10 for the performance of such an operation; any critical data that is temporarily available due to the performance of the cryptographic operation, such as the decrypted secret, the biometrical data, the selection of real points, the hash value constituting the pseudo identity or the like can be erased after the performance of the cryptographic operation has been completed. Such erasure may occur automatically
15 if the security token has no integrated power supply, i.e. no battery, and if the critical data except the encrypted secret is stored in volatile memory such that the critical data is erased automatically when the security token is removed from some external device that provides the power supply. In accordance with an embodiment of the invention the first biometrical data and/or the secret are securely erased from the
20 volatile memory while the power supply is still available. This can be implemented by execution of a program module that executes a respective routine for securely erasing the first biometrical data and/or the secret from a RAM of the security token.

Brief description of the drawings

25

In the following preferred embodiments of the invention will be described in greater detail by way of example only making reference to the drawings in which:

Figure 1 shows a block diagram of an embodiment of a security token being
30 illustrative of encrypting a secret,

Figure 2 is a block diagram of the embodiment of the security token of fig. 1, being illustrative of decrypting the secret,

Figure 3 is a flow chart being illustrative of an embodiment of a method of the invention of assigning a secret to a security token,

Figure 4 is a flow chart being illustrative of an embodiment of a method of the invention of operating a security token for performing a cryptographic operation using the encrypted secret that has been assigned to the security token by the performance of the method of fig. 3,

Figure 5 is a block diagram of an embodiment of a security token of the invention being illustrative of encrypting the secret,

Figure 6 is a flow chart being illustrative of an embodiment of a method of the invention of operating a security token for performing a cryptographic operation using the encrypted secret that has been assigned to the security token by the performance of the method of fig. 5,

Figure 7 is a flow chart of a method of assigning the secret to a security token in accordance with an embodiment of the invention,

Figure 8 is a flow chart being illustrative of an embodiment of a method of the invention of operating a security token for performing a cryptographic operation using the encrypted secret that has been assigned to the security token by the performance of the method of fig. 7.

Detailed description

In the following detailed description like elements of the various embodiments are designated by identical reference numerals.

5

Fig. 1 shows a security token 100, such as a smart card. The security token 100 has an integrated random number generator (RNG) 102 that can generate a random number constituting the secret to be assigned to the security token. The random number generator 102 can be implemented as a pseudo random
10 number generator or as a true physical random number generator, for example by a noise source or a binary symmetric source. In particular, the random number generator 102 can be implemented by software and/or by hardware, such as by means of a shift register with feedback, and/or by a program module that is executed by a processor of the security token 100.

15

The security token 100 has a module 104 for error correction encoding (ECC). The secret provided by the random number generator 102 is entered into the module 104 for error correction encoding of the secret. The module 104 may be implemented by dedicated logical circuitry or by a program module that is
20 executed by the processor of the security token 100.

25

Alternatively, some the functionalities of the module 104 are implemented by a program module and other functionalities of the module 104 are implemented by dedicated logical circuitry, such as by logical circuitry of a crypto coprocessor
116. For example, the crypto coprocessor 116 may include logical circuitry for providing shift functions, polynomial arithmetic functions such as for Reed-Solomon decoding. Such functions can be called by the program module such that the number of time consuming calculations that need to be implemented in software can be reduced.

30

The security token 100 has a logic component 106 for receiving the error corrected encoded secret from the module 104 and of first biometrical data 108 via a communication interface 111. In accordance with an embodiment of the

12a

invention, the logic component 106 can be implemented by means of the crypto coprocessor 116.

In one implementation the biometrical data 108 is acquired by an external sensor, such as a biometric sensor that is coupled to a personal computer or to an external reading device for the security token 100. The externally acquired biometrical raw data is pre-processed such as by the personal computer or the reading device, for example by rounding the biometrical raw data and/or by performing another transformation on the biometrical raw data, such as projecting the biometrical raw data. The resultant biometrical data 108 is then transmitted to the security token 100 and received by the security token 100 by means of its communication interface 111. The communication interface 111 of the security token 100 can be adapted for contact or contactless communication. For example, the communication interface 111 of the security token 100 is a contact or contactless chip card interface, an RFID interface or the like.

In another implementation the security token 100 has an integrated biometric sensor such that the acquisition of the biometric raw data and any pre-processing of the biometric raw data to provide the biometric data 108 is performed by the security token 100 itself.

The logic component 106 performs an XOR operation on the error correction encoded secret received from the module 104 and on the biometric data 108 which provides the template 110 that contains the resultant encrypted secret. The template 110 is stored in non-volatile memory 112 of the security token 100.

The logic component 106 may be implemented by dedicated logic circuitry or by a program module that is executed by the processor of the security token 100.

The security token 100 may comprise a logic component 114 that receives the unencrypted secret from the random number generator 102. The logic component 114 applies a given hashing function onto the secret and outputs a hash value of the secret that can be used as a PI. The PI can be outputted via the communication interface 111 of the security token 100 for external storage. As an alternative or in addition, the PI is stored in non-volatile memory of the security token 100 for later reference.

The logic component 114 can be implemented by dedicated logical circuitry or by a program module that is executed by the processor of the security token 100.

5 It is to be noted that the random number generator 102, the module 104, the logic component 106 and the logic component 114 can be provided by a single processor of the security token 100 that executes respective program instructions. The security token 100 may comprise an additional processor, i.e. crypto coprocessor 116, that implements some or all of these cryptographic
10 functionalities, especially the error correction encoding and/or the transformation of the biometrical raw data to the biometrical data 108.

The secret provided by the random number generator 102, the error correction encoded secret provided by the module 104, the biometrical data 108 and the
15 biometrical raw data, if applicable, as well as the PI are only temporarily stored in the security token 100 such as in a random access memory of the processor or the crypto coprocessor 116 of the security token 100. After the template 110 has been stored in the non-volatile memory 112 and after the PI has been outputted, if applicable, these critical data values are erased from the random
20 access memory. However, for some applications it is preferred to store the PI in non-volatile memory rather than to erase it.

Fig. 2 shows the security token 100 illustrating decryption of the encrypted secret contained in the template 110. The security token 100 has a module 118
25 for error correction decoding of the error correction coding performed by the module 104 shown in Fig. 1. The module 118 may be implemented by dedicated logic circuitry or by a program module that is executed by the processor or the crypto coprocessor 116 of the security token 100.

30 Alternatively, some the functionalities of the module 118 are implemented by a program module and other functionalities of the module 118 are implemented by dedicated logical circuitry, such as by logical circuitry of a crypto coprocessor 116. For example, the crypto coprocessor 116 may include logical circuitry for

14a

providing shift functions, polynomial arithmetic functions such as for Reed-Solomon decoding. Such

functions can be called by the program module such that the number of time consuming calculations that need to be implemented in software can be reduced.

- 5 For decryption of the secret contained in the template 110 biometrical data acquisition is performed of the biometrical feature of the same person from which the biometrical data 108 had been obtained. Due to inaccuracies of the acquisition process the resultant second biometrical data 108' typically is not exactly identical to the original biometrical data 108. For performing the decryption operation the biometrical data 108' and the encrypted secret contained in the template 110 are XORed by
10 the logic component 106 and the resultant codeword is then error correction decoded by the module 118 which provides the correct secret. The secret which is thus recovered can then be used by the security token 100, such as by the crypto coprocessor 116, for performing a cryptographic operation such as for the purposes
15 of authentication, decryption, encryption or generating a digital signature, using the secret as a cryptographic key.

- For example, the person from which the biometrical feature has been obtained needs to enter its PI into the security token 100. The security token 100 compares
20 the PI received via its communication interface 111 to the PI delivered by the logic component 114, i.e. the hash value of the secret. If the received PI and the PI provided by the logic component 114 are identical, authentication of the person is successful such that the functionality of the security token 100 is enabled. For example, after successful authentication of the person the generation of a digital signature is
25 enabled by the security token 100.

Fig. 3 is a flow chart illustrating an embodiment of assigning a secret to a security token.

- 30 In step 200 first biometrical data A is received by the security token either via an external communication interface (cf. communication interface 111 of figs. 1 and 2) or internally from an integrated biometrical sensor of the security token. In step 202 a secret B is defined. For example, the person from which the biometrical data A has been acquired may select the secret B and enter the secret B through the ex-

ternal communication interface into the security token. Alternatively, the secret B can be determined on the occasion of a personalization of the security token and entered into the security token via the external communication interface. Hence, the secret B can be determined outside the security token. Alternatively, the secret B is
5 determined by the security token itself, such as by generating a random number using its internal random number generator (cf. random number generated 102 of fig. 1).

In step 204 an error correction encoding is performed on the secret B to provide the
10 encoded secret b. In step 206 an XOR operation is performed on the error correction encoded secret b and the biometrical data A, such as by performing the XOR operation bitwise which provides the protected template T. In step 208 T is stored in non-volatile memory of the security token and in step 210 the biometrical data A and the secret B are erased from the security token such that only the template T re-
15 mains within the security token as a result of the performance of the assignment of the secret to the security token. It is important to note that the secret B is not stored in any form on the security token but only the template T from which the secret B cannot be recovered unless the biometrical data is acquired from the person.

Hence, the secret B is assigned to the security token without storing the secret B
20 inside the security token or elsewhere.

In accordance with an embodiment of the invention, a hash value of the secret B is generated and output by the security token, such as via its interface 111, in step 202. The hash value is stored in non-volatile memory of the security token.

25 Fig. 4 illustrates the operation for recovering the secret B from the template T. In step 300 second biometrical data A' is received as a result of biometric data acquisition of the biometrical feature of the person from which the original biometrical data A had been acquired. In step 302 an XOR operation is performed on the template T and the biometrical data A' which provides the error correction encoded codeword b' that may contain errors if A' is not identical to A. In step 304 b' is corrected using error correction decoding which provides the correct secret B. In step 306 B can then be used for performing a cryptographic operation. A', b' and B are erased in
30 step 308.

In accordance with an embodiment of the invention, the hash value of the secret B is input into the security token, such as via its interface 111, in step 300 in addition to the biometrical data A'. The received hash value is compared with the hash value stored in the non-volatile memory of the security token.

- 5 Only if the received hash value and the stored hash value are matching the following steps 302 to 308 are executed and a result of the usage of B is returned by the security token via its interface. Otherwise no result is returned.

Fig. 5 shows a block diagram of an alternative embodiment of the security token 100. In contrast to the embodiments of figs. 1 and 2 a polynomial p is used for the encoding. The random number generator 102 delivers a random number, i.e. the secret B, having a number of k digits $b_0, b_1, \dots, b_{k-1}$. Alternatively the secret can be received via the communication interface 111. The security token 100 has a polynomial encoder 120 that uses the k digits of the secret B to
15 determine the coefficients of the polynomial p, i.e.

$$p(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \dots + b_{k-1}x^{k-1}$$

The security token further comprises a calculation module 122 that serves for
20 calculation of the real points that are located on the polynomial p. The real points are calculated by the calculation module 122 using the biometrical data 108 that comprises t values. The polynomial is evaluated at each of the t values to *provide the real points P_i , where $0 < i \leq t$* . This provides the set of real points containing points $P_1 = (x_1, p(x_1))$, $P_2 = (x_2, p(x_2))$, ..., $P_t = (x_t, p(x_t))$.

25 In addition a number of $r - t$ randomly selected stray points are provided by a random number generator 124. The set of real points provided by the calculation module 122 and the set of stray points provided by the random number generator 124 in combination constitute the template 110 containing a
30 number of r points.

It is to be noted that the polynomial encoder 120, the calculation module 122, the random number generator 124, the point selection module 126 and/or the

polynomial decoder 128 can be implemented by dedicated logic circuitry or by a processor of the security token 100, such as by the crypto coprocessor 116, executing respective program modules.

- 5 Fig. 6 shows the security token 100 of fig. 5 illustrating the decryption operation.

The security token 100 has a point selection module 126 for selection of real points from the template 110 and providing the identified real points to a
10 polynomial decoder 128 of the security token 100.

The selection of real points from the template 110 is performed by the point selection module 126 using the biometrical data 108'. The selection of a real point can be performed using a value contained in the biometrical data 108' and
15 searching for a point contained in the template 110 that has a matching or closely matching x-coordinate. If such a point can be identified, this point is considered a real point. This selection process is performed for each one of the values contained in the biometrical data 108' and the resultant identified real points are provided to the polynomial decoder 128 that reconstructs the
20 polynomial b from the real points delivered from the point selection module 126. As the coefficients of the polynomial p constitute the secret B the polynomial decoder 128 thus provides the secret B.

The polynomial decoder 128 may implement Reed Solomon decoding such that
25 even if some of the real points identified by the point selection module 126 are in fact stray points the polynomial p may still be correctly decoded.

Fig. 7 illustrates a respective method of assigning the secret B to the security token using polynomial encoding. In step 400 the biometrical data A having a
30 number of t values is received by the security token. In step 402 the secret B having k digits is received or determined by the security token thus determining the polynomial p having degree k - 1, where t is greater than k for adding redundancy.

In step 404 a real point that is located on the polynomial p is calculated for each value of A and in step 406 a number of $r - t$ stray points that are not located on the polynomial p are added to the set of real points providing a total of r points
5 constituting the template T . The template T is stored in non-volatile memory of the security token in step 408 and the biometrical data A and the secret B are erased from the security token in step 410.

Fig. 8 illustrates the reverse operation: in step 500 the biometrical data A' is
10 received (cf. biometrical data 108' of fig. 6). In step 502 real points contained in T are identified using the values contained in the biometrical data A' . This is performed by searching T for the presence of a point that has a matching or closely matching x-coordinate to a value contained in A' . As a result of step 502
15 points are identified that are in fact real points being located on the polynomial p . Depending on the implementation one or more stray points may wrongly be identified as being real points in step 502; this may occur if a stray point by chance has an x-coordinate that is matching or closely matching a value of A' .

In step 504 the polynomial p is reconstructed using the real points that have
20 been identified in step 502. Depending on the implementation the reconstruction of the polynomial p is even possible if the points identified in step 502 also contain some stray points, in particular if the reconstruction of the polynomial p is performed by means of Reed Solomon decoding.

25 In step 506 the secret B can be used for performing a cryptographic operation and in step 508 the critical data such as A' , B and identification information obtained in step 502 regarding the real points is erased in step 508 from the security token.

30 Analogous to the embodiments of figures 3 and 4, a hash value of the secret B can be stored in the security token, such as in step 400, and the execution of steps 502 to 508 may be subject to receiving the correct hash value of the secret B , such as in step 500.

List of reference numerals

100	Security token
102	Random number generator
104	Module
106	Logic component
108	Biometrical data
108'	Biometrical data
110	Template
111	Communication interface
112	Non-volatile memory
114	Logic component
116	Cryptographic coprocessor
118	Module
120	Polynomial encoder
122	Calculation module
124	Random number generator
126	Point selection module
128	Polynomial decoder

Claims

What is claimed is:

1. A method of operating a security token for performing a cryptographic operation, the security token having assigned thereto a biometrically encrypted secret, the method of operating the security token comprising:

- receiving second biometrical data of a biometrical feature of a person and a pseudo identity by the security token,
- storing the second biometrical data in the security token,
- reading the biometrically encrypted secret from a memory of the security token,
- biometrically decrypting the biometrically encrypted secret so that it becomes a biometrically decrypted secret, using the second biometrical data by the security token,
- comparing the pseudo identity with a hash value of the biometrically decrypted secret,
- using the biometrically decrypted secret for performing the cryptographic operation in case the pseudo identity is identical with the hash value of the biometrically decrypted secret,
- erasing the biometrically decrypted secret and the second biometrical data.

2. The method of claim 1, wherein the secret is used as a key for performing the cryptographic operation.

3. The method of claim 1 or 2, wherein biometrically decrypting the biometrically encrypted secret is performed by performing an XOR operation on the biometrically encrypted secret and the second biometrical data providing an incorrect secret, error correcting the incorrect secret using an error correction code which provides a corrected secret, and further comprising erasing the incorrect secret.

4. The method of claim 1 or 2, the security token having assigned thereto a secret, wherein first biometrical data has a first number (t) of values and the secret has a second number (k) of digits determining coefficients of a polynomial (p), wherein the first number is greater than the second number, wherein a step of biometrically encrypting the secret is performed by calculating a real point for each value of the first biometrical data using the polynomial, and providing random stray points that are not located on the polynomial, wherein a union set of a set of real points and a set of random stray points provides the biometrically encrypted secret, wherein biometrically decrypting the secret is performed by identifying at least a subset of the real points contained in the encrypted secret using the second biometrical data, determining the polynomial using the real points which provides the secret, and further comprising erasing identification information being indicative of the identified real points from the security token.

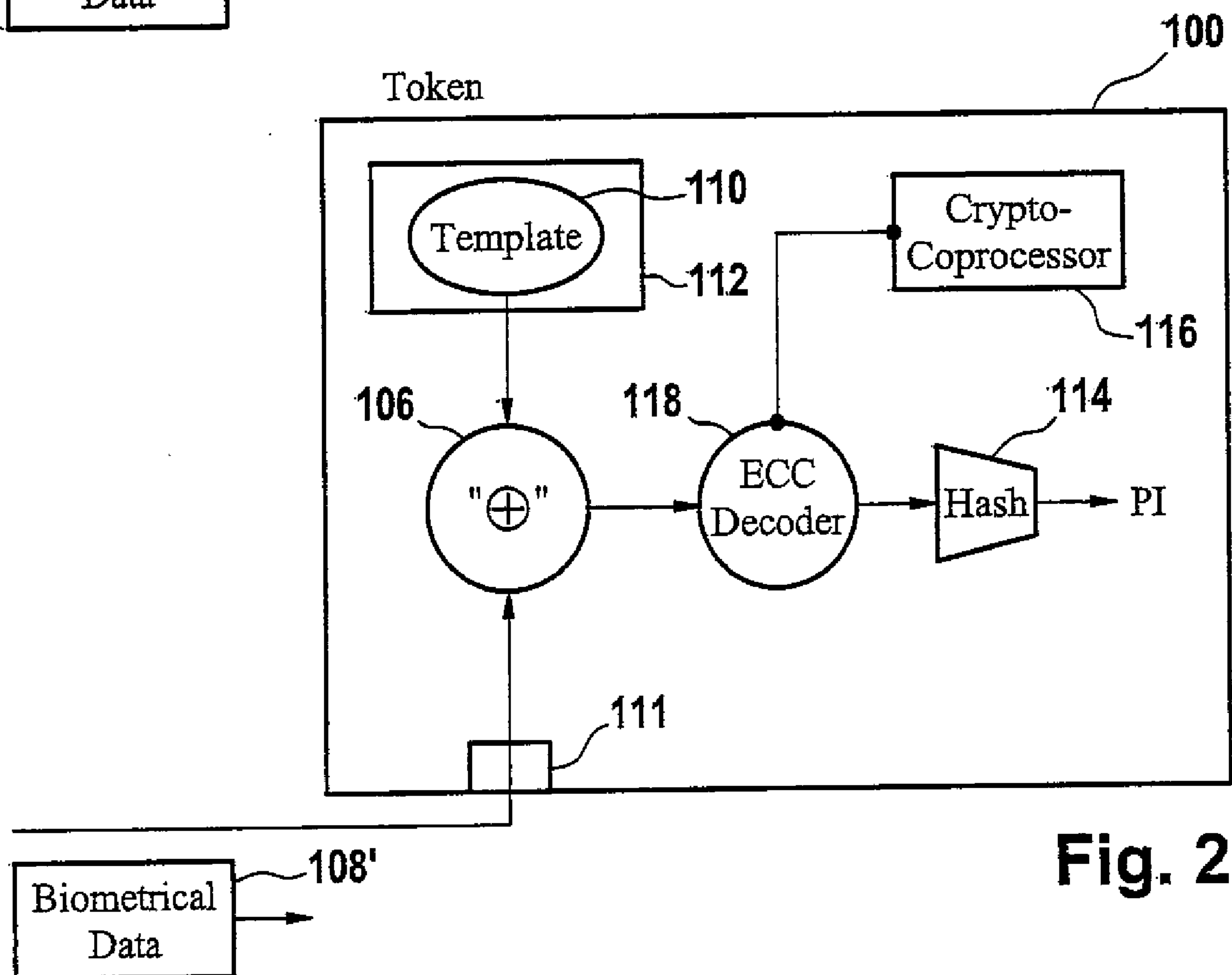
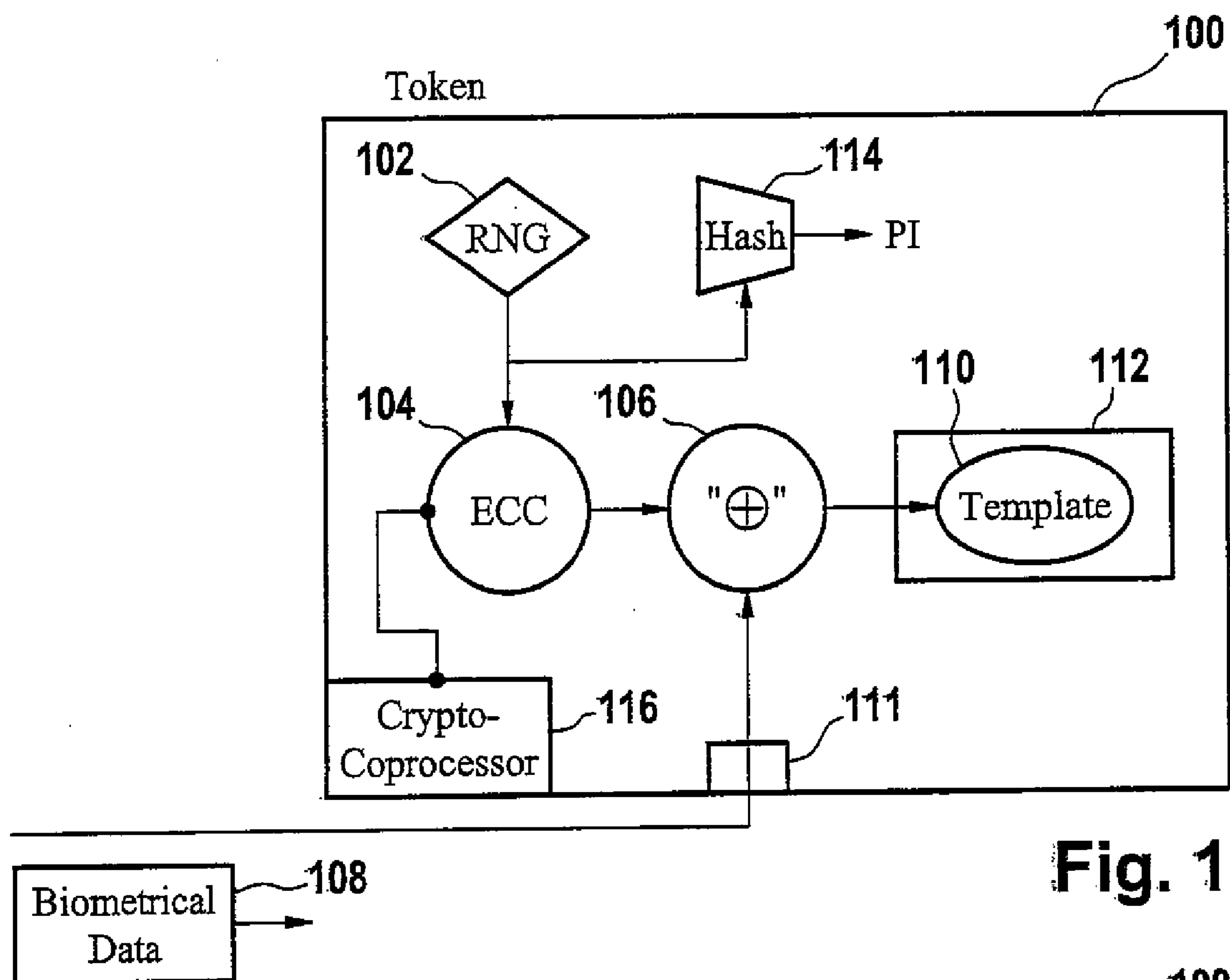
5. A storage medium being readable by a processor of a security token, the storage medium containing instructions that when executed by the processor of the security token cause the security token to perform a method in accordance with any one of claims 1 to 4.

6. A security token comprising:

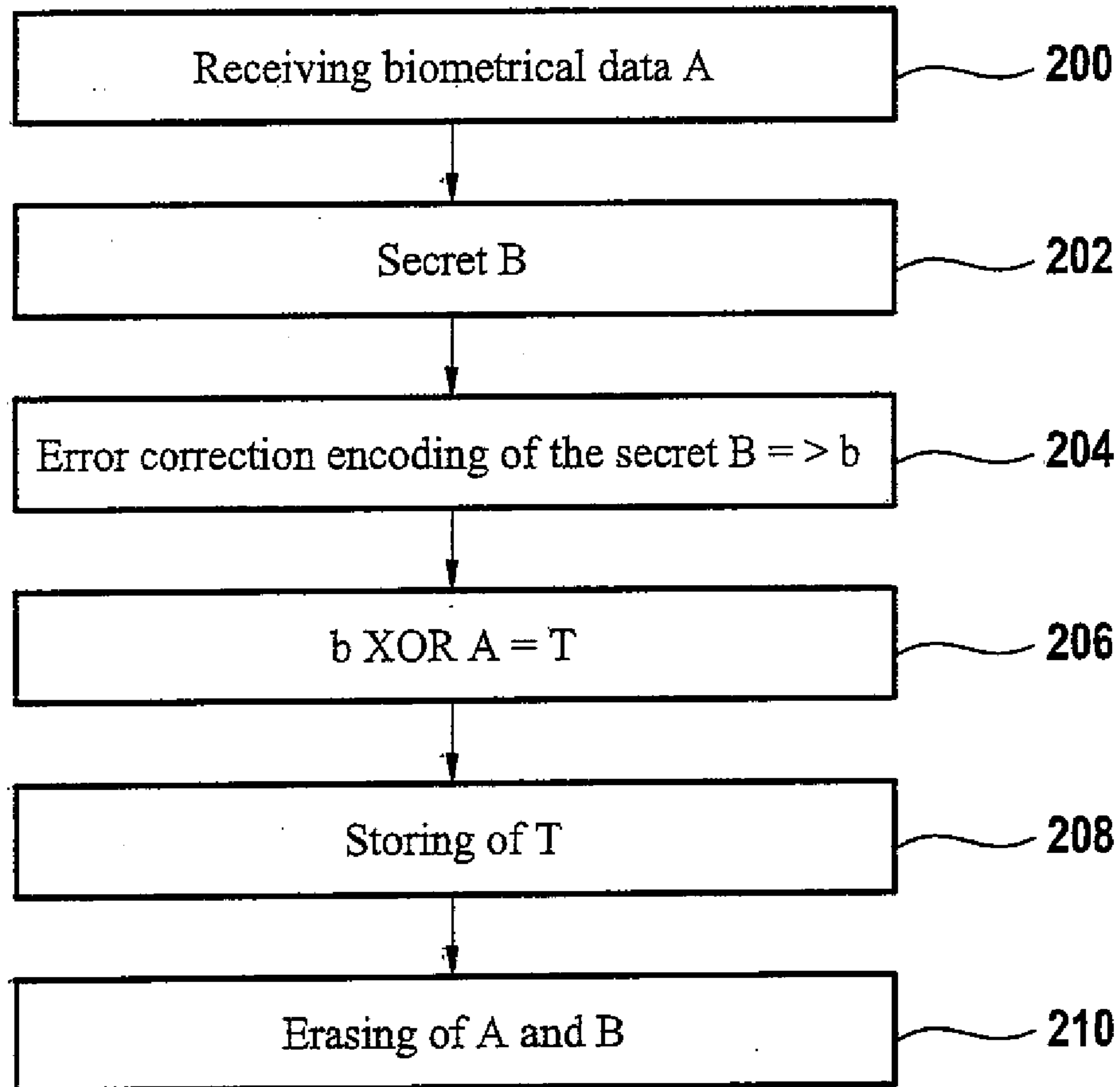
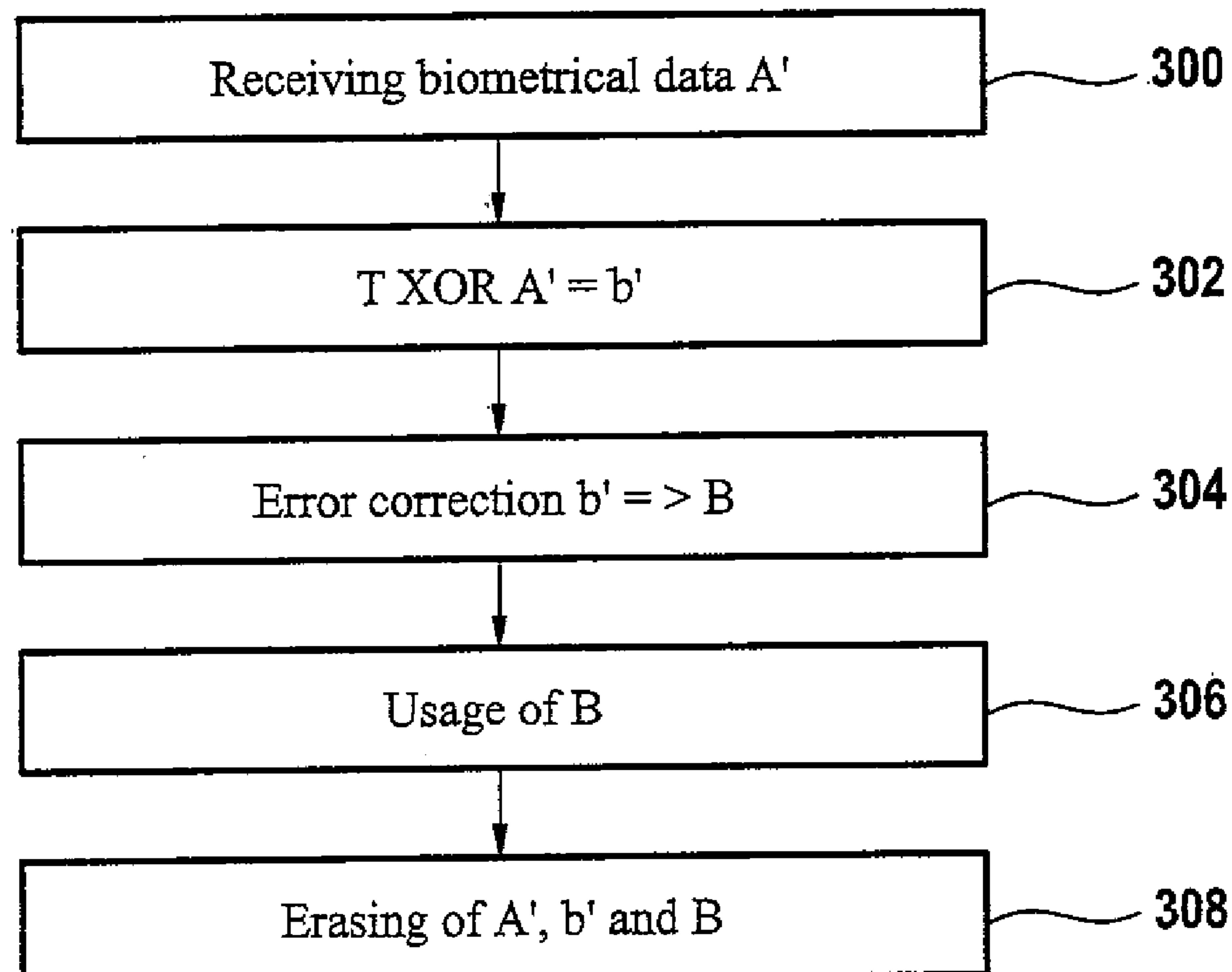
- means for acquiring biometrical data of a biometrical feature of a person,

- means for receiving the biometrical data and a pseudo identity by the security token,
 - volatile storage means for storing the biometrical data in the security token,
 - non-volatile storage means for storing a biometrically encrypted secret,
 - means for reading the biometrically encrypted secret from the non-volatile storage means,
 - means for biometrically decrypting the secret using second biometrical data by the security token,
 - means for generating a hash value of the secret,
 - means for comparing the pseudo identity with the hash value,
 - means for performing a cryptographic operation by using the secret in case the pseudo identity is identical with the hash value of the secret,
 - means for erasing the decrypted secret and the biometrical data from the volatile storage means,
- wherein the biometrical data is acquired from the biometrical feature of a person.

1 / 4



2 / 4

**Fig. 3****Fig. 4**

3 / 4

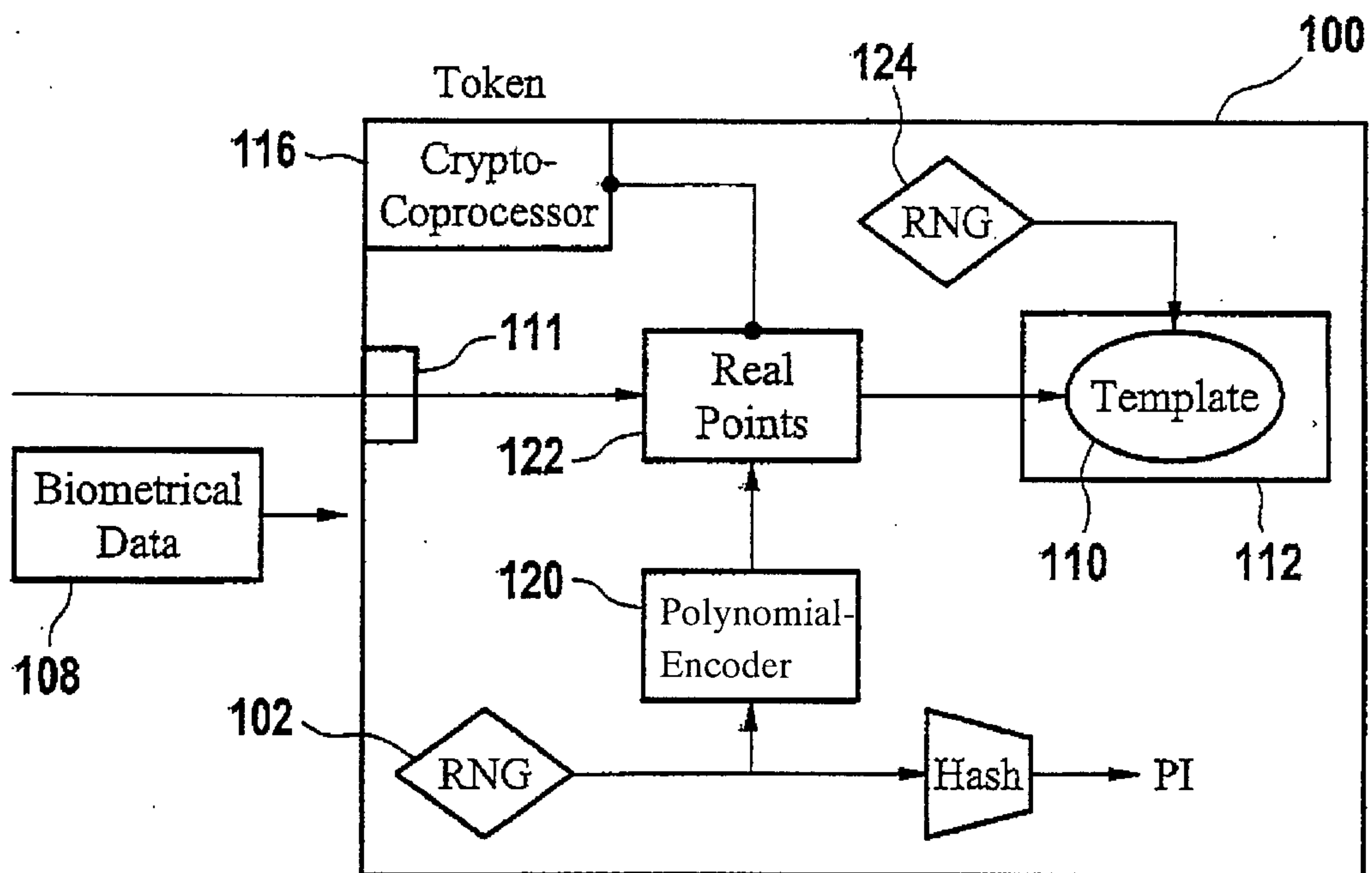


Fig. 5

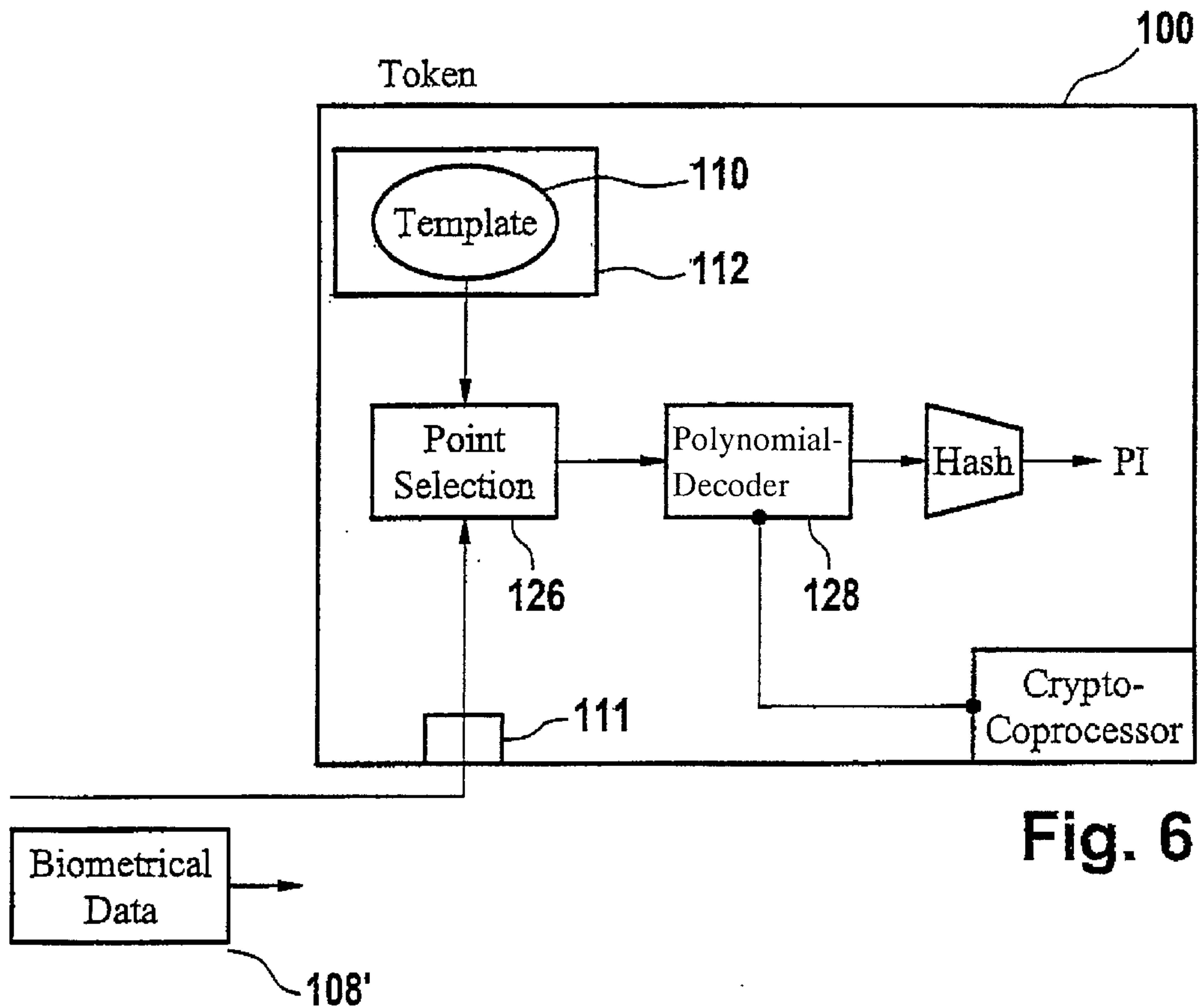
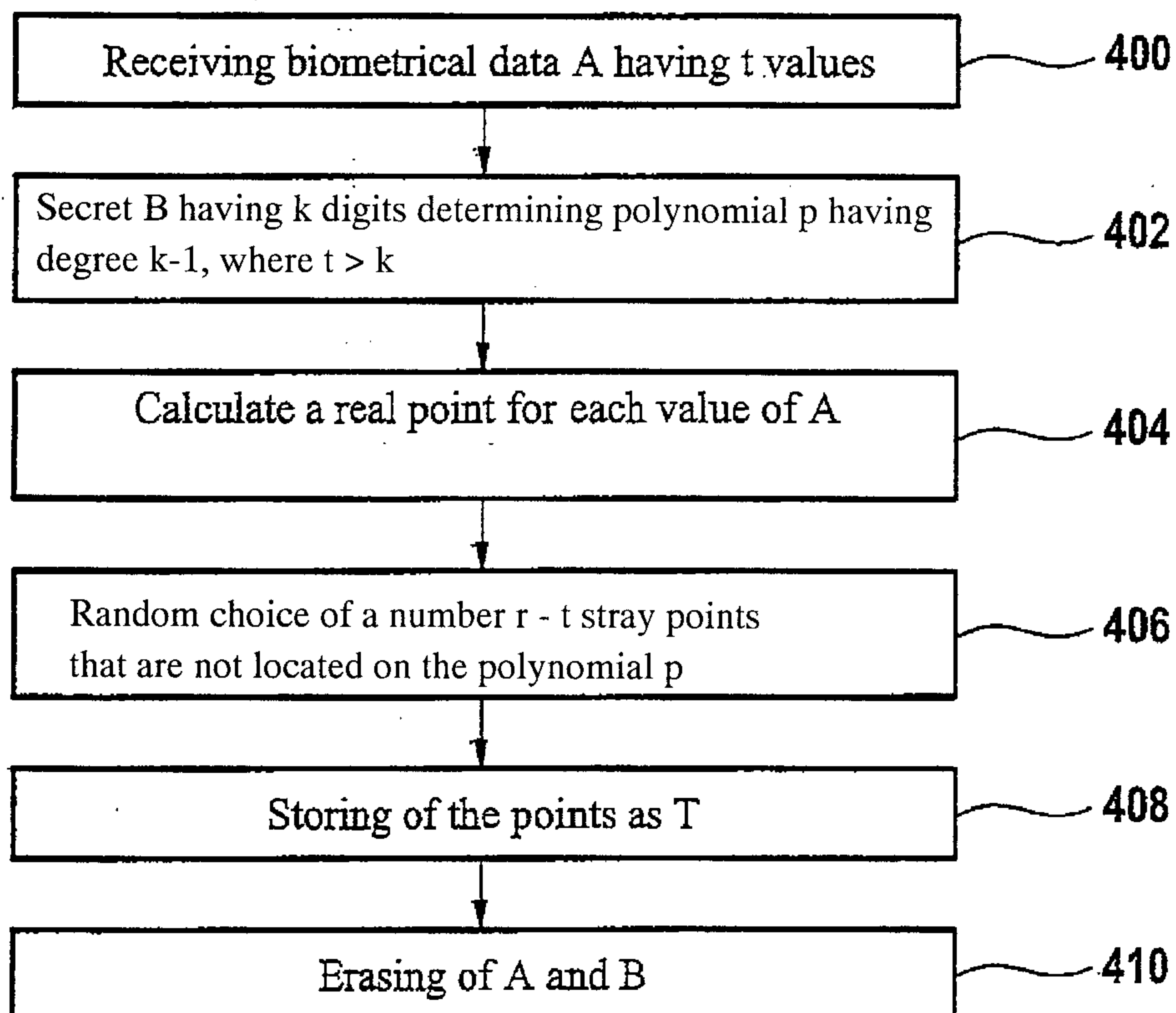
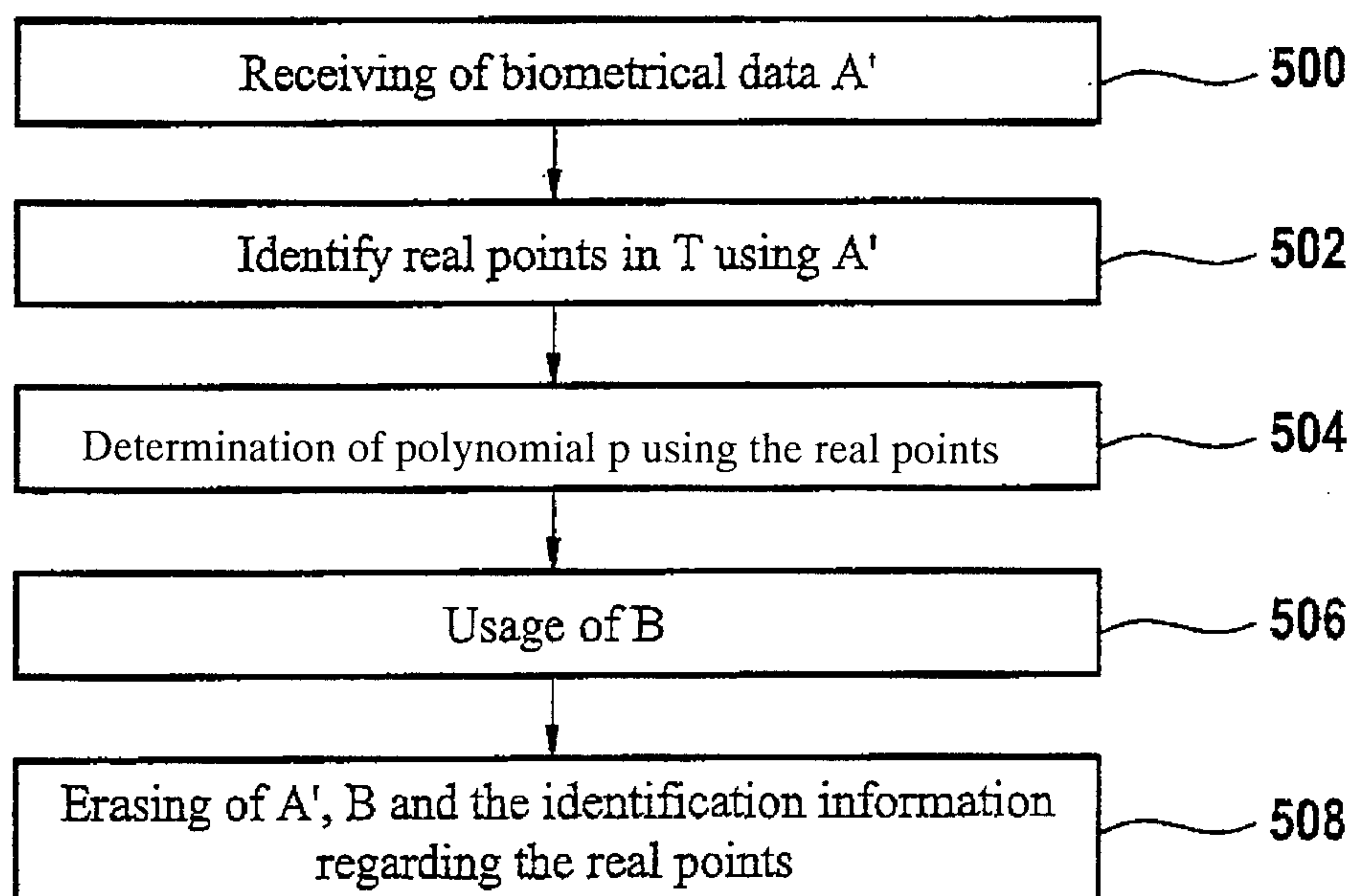


Fig. 6

4 / 4

**Fig. 7****Fig. 8**

