



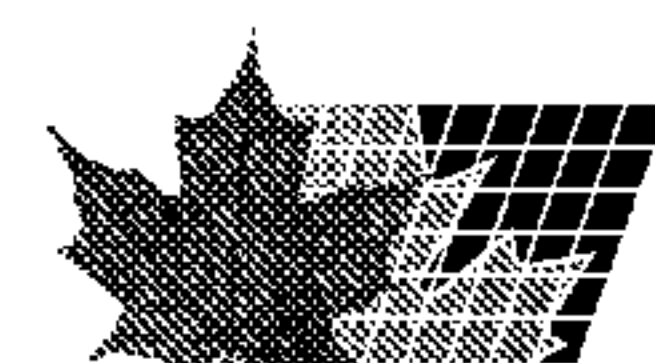
(86) Date de dépôt PCT/PCT Filing Date: 2000/01/27
(87) Date publication PCT/PCT Publication Date: 2000/08/10
(85) Entrée phase nationale/National Entry: 2001/07/25
(86) N° demande PCT/PCT Application No.: FR 00/00188
(87) N° publication PCT/PCT Publication No.: WO 00/46946
(30) Priorités/Priorities: 1999/01/27 (99/01065) FR;
1999/03/23 (99/03770) FR; 1999/10/01 (99/12465) FR;
1999/10/01 (99/12468) FR; 1999/10/01 (99/12467) FR

(51) Cl.Int.⁷/Int.Cl.⁷ H04L 9/32
(71) Demandeurs/Applicants:
TELEDIFFUSION DE FRANCE, FR;
FRANCE TELECOM, FR;
MATH RIZK, BE
(72) Inventeurs/Inventors:
QUISQUATER, JEAN-JACQUES, BE;
GUILLOU, LOUIS, FR
(74) Agent: OYEN WIGGS GREEN & MUTALA

(54) Titre : PROCEDE, SYSTEME, DISPOSITIF DESTINES A PROUVER L'AUTHENTICITE D'UNE ENTITE ET/OU L'INTEGRITE ET/OU L'AUTHENTICITE D'UN MESSAGE
(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY AND/OR THE AUTHENTICITY OF A MESSAGE

(57) **Abrégé/Abstract:**

The proof is provided by the following parameters: m pairs of private values Q_i and public values P_i , $m \geq 1$; a public module n formed by the product of f first factors p_i , $f \geq 2$; a public exponent v, bound by the relationship of the type: $G_i \cdot Q_i^v \sim \text{mod } n$ or $G_i \sim Q_i^v \text{ mod } n$.





DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ : H04L	A2	(11) Numéro de publication internationale: WO 00/46946 (43) Date de publication internationale: 10 août 2000 (10.08.00)															
(21) Numéro de la demande internationale: PCT/FR00/00188 (22) Date de dépôt international: 27 janvier 2000 (27.01.00) (30) Données relatives à la priorité: <table border="0"> <tr> <td>99/01065</td> <td>27 janvier 1999 (27.01.99)</td> <td>FR</td> </tr> <tr> <td>99/03770</td> <td>23 mars 1999 (23.03.99)</td> <td>FR</td> </tr> <tr> <td>99/12465</td> <td>1er octobre 1999 (01.10.99)</td> <td>FR</td> </tr> <tr> <td>99/12467</td> <td>1er octobre 1999 (01.10.99)</td> <td>FR</td> </tr> <tr> <td>99/12468</td> <td>1er octobre 1999 (01.10.99)</td> <td>FR</td> </tr> </table> (71) Déposants (pour tous les Etats désignés sauf US): FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris Cedex 15 (FR). MATH RIZK [BE/BE]; Verte Voie 20, B-1348 Louvain-la-Neuve (BE). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): GUILLOU, Louis [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR). QUISQUATER, Jean-Jacques [BE/BE]; 3, avenue des Canards, B-1640 Rhode Saint Genese (BE).		99/01065	27 janvier 1999 (27.01.99)	FR	99/03770	23 mars 1999 (23.03.99)	FR	99/12465	1er octobre 1999 (01.10.99)	FR	99/12467	1er octobre 1999 (01.10.99)	FR	99/12468	1er octobre 1999 (01.10.99)	FR	(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F-35700 Rennes (FR). (81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Publiée <i>Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.</i>
99/01065	27 janvier 1999 (27.01.99)	FR															
99/03770	23 mars 1999 (23.03.99)	FR															
99/12465	1er octobre 1999 (01.10.99)	FR															
99/12467	1er octobre 1999 (01.10.99)	FR															
99/12468	1er octobre 1999 (01.10.99)	FR															
(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY AND/OR THE AUTHENTICITY OF A MESSAGE (54) Titre: PROCEDE, SYSTEME, DISPOSITIF DESTINES A PROUVER L'AUTHENTICITE D'UNE ENTITE ET/OU L'INTEGRITE ET/OU L'AUTHENTICITE D'UN MESSAGE (57) Abstract The proof is provided by the following parameters: m pairs of private values Q_i and public values P_i , $m > 1$; a public module n formed by the product of f first factors p_i , $f > 2$; a public exponent v, bound by the relationship of the type: $G_i \cdot Q_i^v \equiv \text{mod } n$ or $G_i \equiv Q_i^v \text{ mod } n$. (57) Abrégé La preuve est établie au moyen des paramètres suivants: m couples de valeurs privées Q_i et publiques P_i , $m > 1$, un module public n constitué par le produit de f facteurs premiers p_i , $f > 2$, un exposant public v, liés par des relations du type: $G_i \cdot Q_i^v \equiv 1 \text{ mod } n$ ou $G_i \equiv Q_i^v \text{ mod } n$.																	

Method, system, device designed to prove the authenticity of an entity and/or the integrity and/or the authenticity of a message

The present invention relates to the methods, systems and devices designed to prove the authenticity of an entity and/or the integrity and/or authenticity of a message.

The patent EP 0 311 470 B1, whose inventors are Louis Guillou and Jean-Jacques Quisquater, describes such a method. Hereinafter, reference shall be made to their work by the terms "GQ patent" or "GQ method". Hereinafter, the expression "GQ2", or "GQ2 invention" or "GQ2 technology" shall be used to describe the present invention.

According to the GQ method, an entity known as a "trusted authority" assigns an identity to each entity called a "witness" and computes its RSA signature. In a customizing process, the trusted authority gives the witness an identity and signature. Thereafter, the witness declares the following: *"Here is my identity; I know its RSA signature"*. The witness proves that he knows the RSA signature of his identity without revealing this signature. Through the RSA public identification key distributed by the trusted authority, an entity known as a "controller" ascertains, without obtaining knowledge thereof, that the RSA signature corresponds to the declared identity. The mechanisms using the GQ method run "without transfer of knowledge". According to the GQ method, the witness does not know the RSA private key with which the trusted authority signs a large number of identities.

The GQ method implements modulo computations of numbers comprising 512 bits or more. These computations relate to numbers having substantially the same size raised to powers of the order of $2^{16} + 1$. Now, existing microelectronic infrastructures, especially in the field of bank cards, make use of monolithic self-programmable microprocessors without arithmetical coprocessors. The work load related to the multiple arithmetical applications involved in methods such as the GQ method leads to computation times which, in certain cases, prove to be disadvantageous for consumers using bank cards to pay for their purchases. It may be recalled here that, in seeking to increase the security of payment cards, the banking authorities have raised a problem that is particularly difficult to resolve. Indeed, two apparently contradictory questions have to be resolved: on the one hand, increasing security by using increasingly lengthy and distinct keys for each card while, on the other hand, preventing the work load from leading to excessive computation times for the user. This problem becomes especially acute inasmuch as

it is also necessary to take account of the existing infrastructure and the existing microprocessor components.

The GQ technology described here above makes use of RSA technology. However, while the RSA technology truly depends on the factorization of the modulus n , this dependence is not an equivalence, indeed far from it, as can be seen in what are called "multiplicative attacks" against the various standards of digital signatures implementing the RSA technology.

The goal of the GQ2 technology is twofold: firstly to improve the performance characteristics of RSA technology and secondly to avert the problems inherent in RSA technology. Knowledge of the GQ2 private key is equivalent to knowledge of the factorization of the modulus n . Any attack on the triplets GQ2 leads to the factorization of the modulus n : this time there is equivalence. With the GQ2 technology, the work load is reduced for the signing or self-authenticating entity and for the controller entity. Through a better use of the problem of factorizing in terms of both security and performance, the GQ2 technology averts the drawbacks of RSA technology.

Method

Chinese remainders method applied to the GQ family

More particularly, the invention relates to a method designed to prove the following to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (m being greater than or equal to 1),
- a public modulus n constituted by the product of f prime factors p_1, p_2, \dots, p_f (f being greater than or equal to 2),
- a public exponent v .

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

Said method implements an entity called a witness in the steps defined here below. Said witness entity has f prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private

values Q_i and/or the $f.m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v .

The witness computes commitments R in the ring of integers modulo n . Each commitment is computed by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots, r_f\}$, then by applying the Chinese remainder method.

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments R_i for each of the p_1 values is reduced as compared with what it would have been if the operations had been done modulo n .

The witness receives one or more challenges d . Each challenge d comprises m integers d_i hereinafter called elementary challenges. The witness, on the basis of each challenge d , computes a response D by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

and then by applying the Chinese remainder method.

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments D_i for each of the p_1 values is reduced as compared with what it would have been if the operations had been done modulo n .

The method is such that there are as many responses D as there are challenges d as there are commitments R , each group of numbers R, d, D forming a triplet referenced $\{R, d, D\}$.

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the method according to the invention is designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller. Said demonstrator entity comprises the witness. Said demonstrator and controller entities execute the following steps:

• Step 1: act of commitment R

At each call, the witness computes each commitment R by applying the process specified here above. The demonstrator sends the controller all or part of each commitment R .

• Step 2: act of challenge d

The controller, after having received all or part of each commitment R , produces challenges d whose number is equal to the number of commitments R and sends the challenges d to the demonstrator.

• **Step 3: act of response D**

The witness computes the responses **D** from the challenges **d** by applying the above-specified process.

• **Step 4: act of checking**

5 The demonstrator sends each response **D** to the controller.

First case: the demonstrator has transmitted a part of each commitment R

10 If the demonstrator has transmitted a part of each commitment **R**, the controller, having the **m** public values **G₁, G₂, ..., G_m**, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

15 The controller ascertains that each reconstructed commitment **R'** reproduces all or part of each commitment **R** that has been transmitted to it.

Second case: the demonstrator has transmitted the totality of each commitment R

20 If the demonstrator has transmitted the totality of each commitment **R**, the controller, having the **m** public values **G₁, G₂, ..., G_m**, ascertains that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

25 **Case of the proof of the integrity of the message**

In a second alternative embodiment capable of being combined with a first one, the method of the invention is designed to provide proof to an entity, known as the controller entity, of the integrity of a message **M** associated with an entity called a demonstrator entity. Said demonstrator entity comprises the witness.

30 Said demonstrator and controller entities perform the following steps:

• **Step 1: act of commitment R**

At each call, the witness computes each commitment **R** by applying the process specified here above.

• **Step 2: act of challenge d**

/ The demonstrator applies a hashing function h whose arguments are the message M and all or part of each commitment R to compute at least one token T . The demonstrator sends the token T to the controller. The controller, after having received a token T , produces challenges d equal in number to the number of commitments R and sends the challenges d to the demonstrator.

• **Step 3: act of response D**

The witness computes the responses D from the challenges d by applying the above-specified process.

• **Step 4: act of checking**

The demonstrator sends each response D to the controller. The controller, having the m public values G_1, G_2, \dots, G_m , computes a reconstructed commitment R' , from each challenge d and each response D , this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

Then the controller applies the hashing function h whose arguments are the message M and all or part of each reconstructed commitment R' to reconstruct the token T' . Then the controller ascertains that the token T' is identical to the token T transmitted.

Digital signature of a message and proof of its authenticity

Signing operation

In a third alternative embodiment capable of being combined with either one and/or the other of the other embodiments, the method according to the invention is designed to produce the digital signature of a message M by an entity known as the signing entity. Said signing entity includes the witness.

Said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message M ,
- the challenges d and/or the commitments R ,
- the responses D .

Said signing entity executes the signing operation by implementing the following steps:

• **Step 1: act of commitment R**

At each call, the witness computes each commitment R by applying the process specified here above.

• **Step 2: act of challenge d**

5 The signing entity applies a hashing function h whose arguments are the message M and each commitment R to obtain a binary train. From this binary train, the signing entity extracts challenges d whose number is equal to the number of commitments R .

• **Step 3: act of response D**

10 The witness computes the responses D from the challenges d by applying the above-specified process.

Checking operation

To prove the authenticity of the message M , an entity called a controller checks the signed message. Said controller entity having the signed message carries out a checking operation by proceeding as follows.

15 • **Case where the controller has commitments R , challenges d , responses D**

If the controller has commitments R , challenges d , responses D , the controller ascertains that the commitments R , the challenges d and the responses D satisfy relationships of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

20 or relationships of the type:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

Then the controller ascertains that the message M , the challenges d and the commitments R satisfy the hashing function:

$$d = h(M, R)$$

25 • **Case where the controller has challenges d and responses D**

If the controller has challenges d and responses D , the controller, on the basis of each challenge d and each response D , reconstructs commitments R' satisfying relationships of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

30 or relationships of the type:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

Then the controller ascertains that the message M and the challenges d satisfy the hashing function:

$$d = h(M, R')$$

35 • **Case where the controller has commitments R and responses D**

If the controller has commitments R and responses D , the controller applies the hashing function and reconstructs d'

$$d' = h(M, R)$$

Then the controller device ascertains that the commitments R , the challenges d' and the responses D satisfy relationships of the type

$$R' \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \pmod{n}$$

or relationships of the type:

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \pmod{n}$$

Cases in which the private value Q is chosen first and in which the public value G is deduced from the private value Q

In certain cases, especially to facilitate the production of the pairs of private values Q and public values G , the private value Q is chosen first and the public value G is deduced from the private value Q . More particularly in this case, the method according to the invention is such that the components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,r}$ of the private values Q_i are numbers drawn at random at a rate of one component $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) for each of said prime factors p_j . Said private values Q_i may be computed from said components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,r}$ by the Chinese remainder method. Said public values G_i are computed by performing operations of the following type:

$$G_{i,j} \equiv Q_{i,j}^v \pmod{p_j}$$

Then, in applying the Chinese remainder method to establish G_i such that

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}$$

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments $G_{i,j}$ values for each of the p_j values is reduced as compared with what it would have been if the operations had been done modulo n .

Advantageously, in this case, the method according to the invention is such that the public exponent of verification v is a prime number. It is shown that the security is equivalent to the knowledge of the private value Q_i .

Case in which the public value G is chosen first and in which the private value Q is deduced from the public value G .

Preferably, in this case, said exponent v is such that

$$v = 2^k$$

where k is a security parameter greater than 1.

5 said public value G_i is the square g_i^2 of the base number g_i smaller than the f prime factors p_1, p_2, \dots, p_f ; the base number g_i being such that the two equations:

$$x^2 \equiv g_i \pmod{n} \quad \text{and} \quad x^2 \equiv -g_i \pmod{n}$$

cannot be resolved in x in the ring of integers modulo n and such that the equation:

$$x^v \equiv g_i^2 \pmod{n}$$

can be resolved in x in the ring of the integers modulo n .

10

System

The present invention also relates to a system designed to prove the following to a controller server:

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

15

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (m being greater than or equal to 1),

20

- a public modulus n constituted by the product of said f prime factors p_1, p_2, \dots, p_f (f being greater than or equal to 2),

- a public exponent v .

Said modulus, said exponent and said values are linked by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \quad \text{or} \quad G_i \equiv Q_i^v \pmod{n}.$$

25

Said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card. The witness device comprises a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or $f \cdot m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) of the private values Q_i and of the public exponent v . The witness device also

30

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of integers modulo n .

35

Each commitment is computed by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots, r_f\}$, produced by the random factor production means and then by applying the Chinese remainder method.

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments R_i for each of the p_1 values is reduced as compared with what it would have been if the operations had been done modulo n .

The witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d ; each challenge d comprising m integers d_i hereinafter called elementary challenges.

- computation means, hereinafter called means for the computation of the responses D of the witness device for the computation, on the basis of each challenge d , of a response D of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

and then by applying the Chinese remainder method.

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments D_i for each of the p_1 values is reduced as compared with what it would have been if the operations had been done modulo n .

The witness device also comprises transmission means to transmit one or more commitments R and one or more responses D . There are as many responses D as there are challenges d as there are commitments R , each group of numbers R, d, D forming a triplet referenced $\{R, d, D\}$.

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the system according to the invention is designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

Said system is such that it comprises a demonstrator device associated with a demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said system also comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote

server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

Said system is used to execute the following steps:

5 • **Step 1: act of commitment R**

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means. The demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means.

15 • **Step 2: act of challenge d**

The controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**. The controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

20 • **Step 3: act of response D**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

25 • **Step 4: act of checking**

The transmission means of the demonstrator transmit each response **D** to the controller. The controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,
- 30 - comparison means, hereinafter called the comparison means of the controller device.

First case: the demonstrator has transmitted a part of each commitment R.

If the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values **G₁, G₂, ..., G_m**, compute a reconstructed commitment **R'**, from each

challenge d and each response D , this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

The comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received.

Case where the demonstrator has transmitted the totality of each commitment R

If the transmission means of the demonstrator have transmitted the totality of each commitment R , the computation means and the comparison means of the controller device, having m public values G_1, G_2, \dots, G_m , ascertain that each commitment R satisfies a relationship of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the system according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message M associated with an entity known as a demonstrator. Said system is such that it comprises a demonstrator device associated with the demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said system also comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

Said system is used to execute the following steps:

• **Step 1: act of commitment R**

At each call, the means of computation of the commitments R of the witness device compute each commitment R by applying the process specified here above.

The witness device has means of transmission, hereinafter called transmission means

of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means.

• **Step 2: act of challenge d**

The demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**. The demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device. The controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**. The controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

• **Step 4: act of checking**

The transmission means of the demonstrator transmit each response **D** to the controller. The controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values **G₁**, **G₂**, ..., **G_m**, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**.

The controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

Digital signature of a message and proof of its authenticity

Signing operation

5 In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the system according to the invention is designed to prove the digital signature of a message **M**, hereinafter known as a signed message, by an entity called a signing entity.

The signed message comprises:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

10 Said system is such that it comprises a signing device associated with the signing entity. Said signing device is interconnected with the witness device by interconnection means and may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

15 Said system is used to execute the following steps:

• **Step 1: act of commitment R**

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above.

20 The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means.

• **Step 2: act of challenge d**

25 The signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**.

• **Step 3: act of response D**

30 The means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means. The means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above. The witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device
35 through the interconnection means.

Checking operation

To prove the authenticity of the message **M**, an entity known as the controller checks the signed message.

5 The system comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

10 Said signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means. Thus the controller device has a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- 15 - the responses **D**.

The controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

20 • **Case where the controller device has commitments **R**, challenges **d**, responses **D****

If the controller device has commitments **R**, challenges **d**, responses **D**, the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or relationships of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

30 Then, the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d = h(M, R)$$

• **Case where the controller device has challenges **d** and responses **D****

If the controller has challenges \mathbf{d} and responses \mathbf{D} , the controller reconstructs, on the basis of each challenge \mathbf{d} and each response \mathbf{D} , commitments \mathbf{R}' satisfying relationships of the type

$$\mathbf{R}' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

5 or relationships of the type:

$$\mathbf{R}' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n$$

Then the computation and comparison means of the controller device ascertain that the message \mathbf{M} and the challenges \mathbf{d} satisfy the hashing function:

$$\mathbf{d} = h(\mathbf{M}, \mathbf{R}')$$

10 • Case where the controller has challenges \mathbf{d} and responses \mathbf{D}

If the controller device has challenges \mathbf{d} and responses \mathbf{D} , the computation means of the controller device apply the hashing function and compute \mathbf{d}' such that:

$$\mathbf{d}' = h(\mathbf{M}, \mathbf{R})$$

15 Then the computation and comparison means of the controller device ascertain that the commitments \mathbf{R} , the challenges \mathbf{d}' and the responses \mathbf{D} satisfy relationships of the type:

$$\mathbf{R}' \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \bmod n$$

or relationships of the type:

$$\mathbf{R}' \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot \bmod n$$

20

Case in which the private value \mathbf{Q} is chosen first and in which the public value \mathbf{G} is deduced from the private value \mathbf{Q}

In certain cases, especially to facilitate the production of the pairs of private values \mathbf{Q} and public values \mathbf{G} , the private value \mathbf{Q} is chosen first and the public value \mathbf{G} is deduced from the private value \mathbf{Q} . More particularly in this case, the method according to the invention is such that the components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,r}$ of the private values \mathbf{Q}_i are numbers drawn at random at a rate of one component $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) for each of said prime factors p_j . Said private values \mathbf{Q}_i may be computed from said components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,r}$ by the Chinese remainder method. Said public values \mathbf{G}_i are computed by performing operations of the following type:

30

$$G_{i,j} \equiv Q_{i,j}^v \bmod p_j$$

Then, in applying the Chinese remainder method to establish \mathbf{G}_i such that

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n} ;$$

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments $G_{i,j}$ values for each of the p_j values is reduced as compared with what it would have been if the operations had been done modulo n .

5 Advantageously, in this case, the method according to the invention is such that the public exponent of verification v is a prime number. It is shown that the security is equivalent to the knowledge of the private value Q_i .

10 **Case in which the public value G is chosen first and in which the private value Q is deduced from the public value G .**

Preferably, in this case, said exponent v is such that

$$v = 2^k$$

where k is a security parameter greater than 1. Said public value G_i is the square g_i^2 of the base number g_i smaller than the f prime factors p_1, p_2, \dots, p_f . The
15 base number g_i is such that the two equations:

$$x^2 \equiv g_i \pmod{n} \text{ and } x^2 \equiv -g_i \pmod{n}$$

cannot be resolved in x in the ring of integers modulo n and such that the equation:

$$x^v \equiv g_i^2 \pmod{n}$$

can be resolved in x in the ring of the integers modulo n .

20 **Terminal Device**

Chinese remainder method applied to the GQ family

The invention also relates to a terminal device associated with an entity. The terminal device especially takes the form of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. The terminal device is
25 designed to prove the following to a controller server:

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- 30
- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (m being greater than or equal to 1),
 - a public modulus n constituted by the product of f prime factors p_1, p_2, \dots, p_f (f being greater than or equal to 2),
 - a public exponent v .

Said modulus, said exponent and said values are related by relationships of the type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

Said terminal device comprises a witness device comprising a memory zone
5 containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or $f.m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) of the private values Q_i and of the public exponent v . The witness device also comprises:

- random value production means, hereinafter called random value production
10 means of the witness device,
- computation means, hereinafter called means for the computation of commitments R of the witness device.

The computation means compute commitments R in the ring of the integers modulo n . Each commitment is computed by performing operations of the type:

$$15 \quad R_i \equiv r_i^v \pmod{p_i}$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots, r_f\}$ produced by the random value production means, then by applying the Chinese remainder method.

The witness device also comprises:

- 20 - reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d ; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses D of the witness device, for the computation, on the basis of each
25 challenge d , of a response D , by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \pmod{p_i}$$

and then by applying the Chinese remainder method.

Thus the number of arithmetic operations modulo p_1 to be performed to compute each of the commitments R_i for each of the p_1 values is reduced as
30 compared with what it would have been if the operations had been done modulo n .

Said witness device also comprises transmission means to transmit one or more commitments R and one or more responses D . There are as many responses D as there are challenges d as there are commitments R . Each group of numbers R, d, D forms a triplet referenced $\{R, d, D\}$.

35 Case of the proof of the authenticity of an entity

In a first alternative embodiment, the terminal device according to the invention is designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

Said terminal device is such that it comprises a demonstrator device associated with a demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said demonstrator device also comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

15 • **Step 1: act of commitment R**

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above.

The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means. The demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means.

25 • **Steps 2 and 3: act of challenge d, act of response D**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

30 • **Step 4: act of checking**

The transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the other alternative embodiments, the terminal device according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator. Said terminal device is such that it comprises a demonstrator device associated with the demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said demonstrator device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

• **Step 1: act of commitment **R****

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means.

• **Steps 2 and 3: act of challenge **d**, act of response**

The demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**. The demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T**, through the connection means, to the controller device.

Said controller, after having received the token **T**, produces challenges **d** in a number equal to the number of commitments **R**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means between the demonstrator device and the witness device. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

• **Step 4: act of checking**

The transmission means of the demonstrator send each response **D** to the controller device which performs the check.

Digital signature of a message and proof of its authenticity

Signing operation

5 In a third alternative embodiment, capable of being combined with the others, the terminal device according to the invention is designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity.

The signed message comprises:

- 10
- the message **M**,
 - the challenges **d** and/or the commitments **R**,
 - the responses **D**.

Said terminal device is such that it comprises a signing device associated with the signing entity. Said signing device is interconnected with the witness device by
15 interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said signing device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a controller device associated with the controller entity.
20 Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

• Step 1: act of commitment R

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above.
25 The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means.

• Step 2: act of challenge d

The signing device comprises computation means, hereinafter called the
30 computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**.

• Step 3: act of response D

The means for the reception of the challenges d receive the challenges d coming from the signing device through the interconnection means. The means for computing the responses D of the witness device compute the responses D from the challenges d by applying the process specified here above. The witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses D to the signing device, through the interconnection means.

Controller Device

Chinese remainder method applied to the GQ family

The invention also relates to a controller device. The controller device may especially take the form of a terminal or remote server associated with a controller entity. The controller device is designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (m being greater than or equal to 1),
- a public modulus n constituted by the product of f prime factors p_1, p_2, \dots, p_f (f being greater than or equal to 2),
- a public exponent v .

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

where Q_i designates a private value, unknown to the controller device, associated with the public value G_i .

Case of the proof of the authenticity of an entity

In a first alternative embodiment, capable of being combined with the others, the controller device according to the invention is designed to prove the authenticity of an entity called a demonstrator and an entity called a controller.

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity. Said controller device is used to execute the following steps:

- Steps 1 and 2: act of commitment R , act of challenge d

Said controller device also has means for the reception of all or part of the commitments R coming from the demonstrator device through the connection means.

The controller device has challenge production means for the production, after receiving all or part of each commitment R , of the challenges d in a number equal to the number of commitments R , each challenge d comprising m integers d_i hereinafter called elementary challenges.

The controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means.

• Steps 3 and 4: act of response D , act of checking

The controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,
- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

First case: the demonstrator has transmitted a part of each commitment R .

If the reception means of the controller device have received a part of each commitment R , the computation means of the controller device, having m public values G_1, G_2, \dots, G_m , compute a reconstructed commitment R' , from each challenge d and each response D , this reconstructed commitment R' satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

The comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received.

Second case: the demonstrator has transmitted the totality of each commitment R

If the transmission means of the demonstrator have transmitted the totality of each commitment R , the computation means and the comparison means of the controller device, having m public values G_1, G_2, \dots, G_m , ascertain that each commitment R satisfies a relationship of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

Case of the proof of the integrity of a message

5 In a second alternative embodiment capable of being combined with the others, the controller device according to the invention is designed to prove the integrity of a message **M** associated with an entity known as a demonstrator.

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity. Said controller device is used to execute the following steps:

• Steps 1 and 2: act of commitment R, act of challenge

Said controller device also has means for the reception of tokens **T** coming from the demonstrator device through the connection means. The controller device has challenge production means for the production, after having received the token **T**, of challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers, herein after called elementary challenges. The controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• Steps 3 and 4: act of response D, act of checking

The controller device also comprises means for the reception of the responses **D** coming from the demonstrator device, through the connection means. Said controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values **G₁, G₂, ..., G_m**, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

30 then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**.

The controller device also has comparison means, hereinafter called the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

35 **Digital signature of a message and proof of its authenticity**

In a third alternative embodiment, capable of being combined with other alternative embodiments, the controller device according to the invention is designed to prove the authenticity of the message M by checking the signed message by means of an entity called a controller.

5 The signed message, sent by a signing device associated with a signing entity having a hashing function $h(M, R)$ comprises:

- the message M ,
- the challenges d and/or the commitments R ,
- the responses D .

10 Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity. Said controller device receives the signed message from the signed device, through the connection means.

15 The controller device comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

20 • **Case where the controller device has commitments R , challenges d , responses D**

If the controller has commitments R , challenges d , responses D , the computation and comparison means of the controller device ascertain that the commitments R , the challenges d and the responses D satisfy relationships of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

30 Then the computation and comparison means of the controller device ascertain that the message M , the challenges d and the commitments R satisfy the hashing function:

$$d = h(M, R)$$

• **Case where the controller device has challenges d and responses D**

If the controller device has challenges \mathbf{d} and responses \mathbf{D} , the computation means of the controller device, on the basis of each challenge \mathbf{d} and each response \mathbf{D} , compute commitments \mathbf{R}' satisfying relationships of the type

$$\mathbf{R}' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

5 or relationships of the type:

$$\mathbf{R}' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n$$

Then the computation and comparison means of the controller device ascertain that the message \mathbf{M} and the challenges \mathbf{d} satisfy the hashing function:

$$\mathbf{d} = h(\mathbf{M}, \mathbf{R}')$$

10 • **Case where the controller device has commitments \mathbf{R} and responses \mathbf{D}**

If the controller device has commitments \mathbf{R} and responses \mathbf{D} , the computation means of the controller device apply the hashing function and compute \mathbf{d}' such that

$$\mathbf{d}' = h(\mathbf{M}, \mathbf{R})$$

15 Then the computation and comparison means of the controller device ascertain that the commitments \mathbf{R} , the challenges \mathbf{d}' and the responses \mathbf{D} satisfy relationships of the type:

$$\mathbf{R} \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \bmod n$$

or relationships of the type:

$$\mathbf{R} \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot \bmod n$$

20 **Detailed description of the alternative embodiment when the public exponent $v = 2^k$**

Description

The goal of GQ technology may be recalled: it is the dynamic authentication of entities and associated messages as well as the digital signature of messages.

5 The standard version of GQ technology makes use of RSA technology. However, although the RSA technology truly depends on factorizing, this dependence is not an equivalence, far from it, as can be shown from attacks, known as multiplicative attacks, against various digital signature standards implementing RSA technology.

10 In the context of GQ2 technology, the present part of the invention relates more specifically to the use of sets of GQ2 keys in the context of dynamic authentication and digital signature. The GQ2 technology does not use RSA technology. The goal is a twofold one: first, to improve performance with respect to RSA technology and secondly to prevent problems inherent in RSA technology. The GQ2 private key is
15 the factorization of the modulus n . Any attack on the GQ2 triplets amounts to the factorizing of the modulus n : this time there is equivalence. With the GQ2 technology, the work load is reduced both for the entity that signs or is authenticated and for the one that checks. Through an improved use of the problem of factorization, in terms of both security and performance, the GQ2 technology rivals
20 the RSA technology.

The GQ2 technology uses one or more small integers greater than 1, for example m small integers ($m \geq 1$) called base numbers and referenced g_i . Since the base numbers are fixed from g_1 to g_m with $m > 1$, a public verification key $\langle v, n \rangle$ is chosen as follows. The public verification exponent v is 2^k where k is a small integer
25 greater than 1 ($k \geq 2$). The public modulus n is the product of at least two prime factors greater than the base numbers, for example f prime factors ($f \geq 2$) referenced by p_j , from $p_1 \dots p_f$. The f prime factors are chosen so that the public modulus n has the following properties with respect to each of the m base numbers from g_1 to g_m .

- Firstly, the equations (1) and (2) cannot be resolved in x in the ring of the integers modulo n , that is to say that g_i and $-g_i$ are two non-quadratic residues (mod n).

$$x^2 \equiv g_i \pmod{n} \quad (1)$$

$$x^2 \equiv -g_i \pmod{n} \quad (2)$$

- Secondly, the equation (3) can be resolved in x in the ring of the integers modulo n .

$$x^{2^k} \equiv g_i^2 \pmod{n} \quad (3)$$

Since the public verification key $\langle v, n \rangle$ is fixed according to the base numbers from g_1 to g_m with $m \geq 1$, each base number g_i determines a pair of GQ2 values comprising a public value G_i and a private value Q_i : giving m pairs referenced $G_1 Q_1$ to $G_m Q_m$. The public value G_i is the square of the base number g_i : giving $G_i = g_i^2$. The private value Q_i is one of the solutions to the equation (3) or else the inverse (mod n) of such a solution.

Just as the modulus n is broken down into f prime factors, the ring of the integers modulo n are broken down into f Galois fields, from $CG(p_1)$ to $CG(p_f)$. Here are the projections of the equations (1), (2) and (3) in $CG(p_j)$.

$$x^2 \equiv g_i \pmod{p_j} \quad (1.a)$$

$$x^2 \equiv -g_i \pmod{p_j} \quad (2.a)$$

$$x^{2^k} \equiv g_i^2 \pmod{p_j} \quad (3.a)$$

Each private value Q_i can be represented uniquely by f private components, one per prime factor: $Q_{ij} \equiv Q_i \pmod{p_j}$. Each private component Q_{ij} is a solution to the equation (3.a) or else the inverse (mod p_j) of such a solution. After all the possible solutions to each equation (3.a) have been computed, the Chinese remainder technique sets up all the possible values for each private value Q_i on the basis of f components of $Q_{i,1}$ to $Q_{i,f}$: $Q_i = \text{Chinese remainders}(Q_{i,1}, Q_{i,2}, \dots, Q_{i,f})$ so as to obtain all the possible solutions to the equation (3).

The following is the Chinese remainder technique: let there be two positive integers that are mutually prime numbers a and b such that $0 < a < b$, and two components X_a from 0 to $a-1$ and X_b from 0 to $b-1$. It is required to determine $X = \text{Chinese remainders}(X_a, X_b)$, namely the unique number X from 0 to $a.b-1$ such that $X_a \equiv X \pmod{a}$ and $X_b \equiv X \pmod{b}$. The following is the Chinese remainder parameter: $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. The following is the Chinese remainder operation: $\varepsilon \equiv X_b \pmod{a}$; $\delta = X_a - \varepsilon$; if δ is negative, replace δ by $\delta + a$; $\gamma \equiv \alpha \cdot \delta \pmod{a}$; $X = \gamma \cdot b + X_b$.

When the prime factors are arranged in rising order, from the smallest p_1 to the greatest p_f , the Chinese remainder parameters can be the following (there are $f-1$ of them, namely one less than prime factors). The first Chinese remainder parameter is $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. The second Chinese remainder parameter is $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. The i -th Chinese remainder parameter is $\lambda \equiv \{p_1.p_2 \dots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. And so on and so forth. Finally, in $f-1$ Chinese remainder

operations, a first result (mod p_2 times p_1) is obtained with the first parameter and then a second result (mod $p_1.p_2$ times p_3) with the second parameter and so on and so forth until a result (mod $p_1. \dots p_{f-1}$ times p_f), namely (mod n).

There are several possible representations of the private key GQ2, which expresses the **polymorphous nature of the private key GQ2**. The various representations prove to be equivalent: they all amount to knowledge of the factorization of the module n which is the true private GQ2 key. If the representation truly affects the behavior of the signing entity or self-authenticating entity, it does not affect the behavior of the controller entity.

Here are the main three possible representations of the GQ2 private key.

1) The standard representation in GQ technology consists of the storage of m private values Q_i and the public verification key $\langle v, n \rangle$; in GQ2, this representation is rivalled by the following two. 2) The optimal representation in terms of work load consists in storing the public exponent v , the f prime factors p_j , $m.f$ private components Q_{ij} and $f-1$ parameters of the Chinese remainders. 3) The optimal representation in terms of private key size consists in storing the public exponent v , the m basic numbers g_i and the f prime factors p_j , then in starting each use by setting up either m private values Q_i and the module n to return to the first representation or else $m.f$ private components $Q_{i,j}$ and $f-1$ parameters of the Chinese remainders to return to the second one.

The signing or self-authenticating entities can all use the same base numbers. Unless otherwise indicated, the m base numbers from g_1 to g_m can then advantageously be the m first prime numbers;

Because the security of the dynamic authentication mechanism or digital signature mechanism is equivalent to knowledge of a breakdown of the modulus, the GQ2 technology cannot be used to simply distinguish two entities using the same modulus. Generally, each entity that authenticates itself or signs has its own GQ2 modulus. However, it is possible to specify GQ2 moduli with four prime factors, two of which are known by an entity and the other two by another entity.

Here is a first set of GQ2 keys with $k = 6$, giving $v = 64$, $m = 3$, giving three base numbers: $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, and $f = 3$, namely a modulus with three prime factors: two congruent to 3 (mod 4) and one to 5 (mod 8). It must be noted that $g = 2$ is incompatible with a prime factor congruent to 5 (mod 8).

$p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833$

$p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B$

$p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD$
 $n = p_1 \cdot p_2 \cdot p_3 = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9$
 $02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144$
 $CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD$

5 $Q_{1,1} = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE$

$Q_{2,1} = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89$

$Q_{3,1} = 6FB3B9C05A03D7CADA9A3425571EF5ECC54D7A7B6F$

$Q_{1,2} = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502$

$Q_{2,2} = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E$

10 $Q_{3,2} = FDC4A8E53E185A4BA793E93BEE5C636DA731BDCA4E$

$Q_{1,3} = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE$

$Q_{2,3} = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877$

$Q_{3,3} = 01682D490041913A4EA5B80D16B685E4A6DD88070501$

$Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8$

15 $C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A$
 $C74D9743435AB4D7CF0FF6557$

$Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4$

$DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8$

$82288273ADE67353A5BC316C093$

20 $Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A$

$AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197$

$697238537FE7A0195C5E8373EB74D$

The following is a second set of GQ2 keys, with $k = 9$, that is $v = 512$, $m = 2$, that is
 two base numbers: $g_1 = 2$ and $g_2 = 3$, and $f = 3$, giving a modulus with three prime
 25 factors congruent to 3 (mod 4).

$p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB$

$p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7$

$p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3$

$n = p_1 \cdot p_2 \cdot p_3 = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D$

30 $6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49$

$761B276A8E6B6977A21D51669D039F1D7$

$Q_{1,1} = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1$

$Q_{2,1} = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E$

$Q_{1,2} = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A$

$Q_{2,2} = 045ECB881387582E7C556887784D2671CA118E22FCF2$

$Q_{1,3} = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982$

5 $Q_{2,3} = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB$

$Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C$
 $35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6$
 $EDDA092D0CF108D0AB708405DA46$

10 $Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64$
 $9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6$
 $F11F19874DE7DC5D1DF2A9252D$

Dynamic authentication

15 The dynamic authentication mechanism is designed to prove, to an entity known as a **controller**, the authenticity of another entity known as a **demonstrator** as well as the authenticity of a possible associated message M , so that the controller can be sure that it is truly the demonstrator and, as the case may be, only the demonstrator and that the demonstrator is truly speaking of the same message M . The associated message M is optional. This means that it may be empty.

20 The dynamic authentication mechanism is a sequence of four acts: an act of commitment, an act of challenge, an act of response and an act of checking. The demonstrator fulfills the acts of commitment and response. The controller fulfills the acts of challenge and control.

25 Within the demonstrator, it is possible to isolate a witness so as to isolate the most sensitive parameters and functions of the demonstrator, namely the production of commitments and responses. The witness has the parameter k and the private key $GQ2$, namely the factorization of the module n according to one of the three representations referred to here above: • the f prime factors and the m base numbers, • the $m.f$ private components, the f prime factors and the $f-1$ parameters of the Chinese remainders, • the m private values and the modulus n .

30 The witness may correspond to a partial embodiment, for example, • a chip card connected to a PC forming the entire demonstrator or again, • specially protected programs within a PC, or again, • specially protected programs within a smart card. The witness thus isolated is similar to the witness defined here below

within the signing entity. At each execution of the mechanism, the witness produces one or more commitments R and then as many responses D to as many challenges d . Each set $\{R, d, D\}$ is a **GQ2 triplet**.

5 Apart from comprising the witness, the demonstrator also has, if necessary, a hashing function and a message M .

The controller has the modulus n and the parameters k and m ; if necessary, it also has the same hashing function and a message M . The controller is capable of reconstituting a commitment R' from any challenge d and any response D . The parameters k and m inform the controller. Failing any indication to the contrary, the
10 m base numbers from g_1 to g_m are the m first prime numbers. Each challenge d must have m elementary challenges referenced from d_1 to d_m : one per base number. This elementary challenge from d_1 to d_m may take a value of 0 to $2^{k-1}-1$ (the values of $v/2$ to $v-1$ are not used). Typically, each challenge is encoded by m times $k-1$ bits (and not by m times k bits). For example, $k = 6$ and $m = 3$ and the base numbers 3, 5
15 and 7, each challenge has 15 bits transmitted on two bytes; with $k = 9$, $m = 2$ and the base numbers 2 and 3, each challenge has 16 bits transmitted on two bytes. When the $(k-1).m$ possible challenges are also possible, the value $(k-1).m$ determines the security provided by each GQ2 triplet: an impostor who, by definition, does not know the factorization of the module n has exactly one chance of success in $2^{(k-1).m}$.
20 When $(k-1).m$ is equal to 15 to 20, one triplet is enough to reasonably provide for dynamic authentication. To achieve any security level whatsoever, it is possible to produce triplets in parallel. It is also possible to produce them sequentially, namely to repeat the execution of the mechanism.

1) **The act of commitment** comprises the following operations.

25 When the witness has m private values from Q_1 to Q_m and the modulus n , it draws one or more random values r ($0 < r < n$) at random and privately; then by k successive squaring (mod n) operations, it converts each random value r into a commitment R .

$$R \equiv r^v \pmod{n}$$

30 Here is an example with the first set of keys with $k = 6$.

$r = \text{B8AD426C1AC0165E94B894AC2437C1B1797EF562CFA53A4AF8}$
43131FF1C89CFDA131207194710EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

$R = \text{FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56}$
35 D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04

49CC4292E5DD2BDB00828AF18

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij} , it draws one or more collections of f random values at random and privately: each collection has one random value r_i per prime factor p_i ($0 < r_i < p_i$); then by k successive operations of squaring (mod p_i), it converts each random value

$$R_i \equiv r_i^v \pmod{n}$$

Here is an example with the second set of keys with $k = 9$.

$r_1 = \text{B0418EABEBADF0553A28903F74472CD49EE8C82D86}$

10 $R_1 = \text{022B365F0BEA8E157E94A9DEB0512827FFD5149880F1}$

$r_2 = \text{75A8DA8FE0E60BD55D28A218E31347732339F1D667}$

$R_2 = \text{057E43A242C485FC20DEEF291C774CF1B30F0163DEC2}$

$r_3 = \text{0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27}$

$R_3 = \text{06E14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C}$

15 For each collection of f commitment components, the witness sets up a commitment according to the technique of Chinese remainders. There are as many commitments as there are collections of random values.

$$R = \text{Chinese reminders } (R_1, R_2, \dots, R_j)$$

$R = \text{28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7}$

20 $\text{D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9}$

$\text{9123B56446F6C928736B17B4BA4A529}$

In both cases, the demonstrator sends the controller all or part of each commitment R , or at least a hashing code H obtained by hashing each commitment R and one message M .

25 **2) The act of challenge** consists in drawing at random one or more challenges d each consisting of m elementary challenges d_1, d_2, \dots, d_m ; each elementary challenge d_i takes one of the values from 0 to $v/2-1$.

$$d = d_1, d_2, \dots, d_m$$

Here is an example for the first set of keys with $k = 6$ and $m = 3$.

30 $d_1 = 10110 = 22 = '16'; d_2 = 00111 = 7; d_3 = 00010 = 2$

$$d = 0 \parallel d_1 \parallel d_2 \parallel d_3 = 01011000 \ 11100010 = 58 \text{ E2}$$

Here is an example for the second set of keys with $k = 9$ and $m = 2$.

$$d = d_1 \parallel d_2 = 58 \text{ E2, that is, in decimal notation 88 and 226}$$

The controller transmits each challenge d to the demonstrator.

35 **3) The act of response** has the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n , it computes one or more responses D in using each random value r of the act of commitment and the private values according to the elementary challenges.

$$\begin{aligned} X &\equiv Q_1^{d_1} \cdot Q_2^{d_2} \dots Q_m^{d_m} \pmod{n} \\ D &\equiv r \cdot X \pmod{n} \end{aligned}$$

Here is an example for the first set of keys.

$D = \text{FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386}$
 $5\text{EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480}$
 $10 \quad \text{A2C6A290273479FEC9171990A17}$

When the witness has f prime factors from p_i to p_f and $m \cdot f$ private components $Q_{i,j}$, it computes one or more collections of f response components in using each collection of random values of the act of commitment: each collection of response components comprises one component per prime factor.

$$\begin{aligned} X_i &\equiv Q_{1,i}^{d_1} \cdot Q_{2,i}^{d_2} \dots Q_{m,i}^{d_m} \pmod{p_i} \\ D_i &\equiv r_i \cdot X_i \pmod{p_i} \end{aligned}$$

Here is an example for the second set of keys.

$D_1 = r_1 \cdot Q_{1,1}^{d_1} \cdot Q_{2,1}^{d_2} \pmod{p_1} =$
 $02660ADF3C73B6DC15E196152322DDE8EB5B35775E38$
 $20 \quad D_2 = r_2 \cdot Q_{1,2}^{d_1} \cdot Q_{2,2}^{d_2} \pmod{p_2} =$
 $04C15028E5FD1175724376C11BE77052205F7C62AE3B$
 $D_3 = r_3 \cdot Q_{1,3}^{d_1} \cdot Q_{2,3}^{d_2} \pmod{p_3} =$
 $0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52$

For each collection of response components, the witness draws up a response according to the Chinese remainder technique. There are as many responses as there are challenges.

$D = \text{Chinese remainders } (D_1, D_2, \dots, D_f)$
 $D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36$
 $4\text{CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00}$
 $30 \quad 195A7305C6FF3323F72DC1AB$

In both cases, the demonstrator sends each response D to the controller.

4) **The checking act** consists in ascertaining that each triplet $\{R, d, D\}$ verifies an equation of the following type for a non-zero value,

$$R \cdot \prod_{i=1}^m G_i^{d_i} \equiv D^{2^t} \pmod{n} \text{ or else } R \equiv D^{2^t} \cdot \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

or else in setting up each commitment: none should be zero.

$$R' \equiv D^{2^t} / \prod_{i=1}^m G_i^{d_i} \pmod{n} \text{ or else } R' \equiv D^{2^t} \cdot \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

5 If necessary, the controller then computes a hashing code H' in hashing each re-established commitment R' and a message M' . The dynamic authentication is successful when the controller thus retrieves what it had received at the end of the first act of commitment, namely all or part of each commitment R , or else the hashing code H .

10 For example, a sequence of elementary operations converts the response D into a commitment R' . The sequence has k squares (mod n) separated by $k-1$ divisions or multiplications (mod n) by base numbers. For the i -th division or multiplication, which is performed between the i -th square and the $i+1$ st square, the i -th bit of the elementary challenge d_i indicates whether it is necessary to use g_i , the i -th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2 , ...
15 up to the i -th bit of the elementary challenge d_m which indicates whether it is necessary to use g_m .

Here is an example for the first set of keys.

$D^2 \pmod{n} = \text{FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3}$
 $2\text{B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7}$
 20 $\text{FDA95D5BD6347DC8B978CA217733}$
 $3 \cdot D^2 \pmod{n} = \text{F739B708911166DFE715800D8A9D78FC3F332FF622D}$
 $3\text{EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF}$
 $987041B4852890D83FC6B48D3EF6A9DF$
 $3^2 \cdot D^4 \pmod{n} = \text{682A7AF280C49FE230BEE354BF6FFB30B7519E3C8}$
 25 $92\text{DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF}$
 $8826635790743EA7D9A15A33ACC7491D4A7$
 $3^4 \cdot D^8 \pmod{n} = \text{BE9D828989A2C184E34BA8FE0F384811642B7B548F}$
 $870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3}$
 $939E69D413F0BABC6DEC441974B1A291$
 30 $3^5 \cdot 5 \cdot D^8 \pmod{n} = \text{2B40122E225CD858B26D27B768632923F2BBE5}$
 $\text{DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D}$
 $4\text{AC1E89C2235C363830EBF4DB42CEA3DA98CFE00}$
 $3^{10} \cdot 5^2 \cdot D^{16} \pmod{n} = \text{BDD3B34C90ABBC870C604E27E7F2E9DB2D383}$
 $68\text{EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD}$

B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} \cdot 5^3 \cdot 7 \cdot D^{16} \pmod n = \text{DBFA7F40D338DE4FBA73D42DBF427BBF195}$
 $\text{C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444}$
 $\text{A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F}$

5 $3^{22} \cdot 5^6 \cdot 7^2 \cdot D^{32} \pmod n = \text{C60CA9C4A11F8AA89D9242CE717E3DC6C1}$
 $\text{A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A}$
 $\text{EECB70509667A3CB052029C94EDF27611FAE286A7}$

$3^{22} \cdot 5^7 \cdot 7^2 \cdot D^{32} \pmod n = \text{DE40CB6B41C01E722E4F312AE7205F18CDD}$
 $\text{0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77}$

10 $\text{886F4AC5222F9C863DACA440CF5F1A8E374807AC}$

$3^{44} \cdot 5^{14} \cdot 7^4 \cdot D^{64} \pmod n$, namely, $3^{2^C} \cdot 5^E \cdot 7^4 \cdot D^{40} \pmod n$ with the exponents in
 hexadecimal notation = $\text{FFDD736B666F41FB771776D9D50DB7CDF03F3D9}$
 $\text{76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C}$
 $\text{21210C6B0449CC4292E5DD2BDB00828AF18}$

15 We find the commitment R . The authentication is successful.

Here is an example for the second set of keys.

$D^2 \pmod n = \text{C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E}$
 $\text{24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC}$
 $\text{693F8395ACEF9206B172A8A2C2CCBB}$

20 $3 \cdot D^2 \pmod n = \text{534C6114D385C3E15355233C5B00D09C2490D1B8D8E}$
 $\text{D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20}$
 $\text{1D6D138F3999FC1D06A2B2647D48283}$

$3^2 \cdot D^4 \pmod n = \text{A9DC8DEA867697E76B4C18527DFFC49F4658473D03}$
 $\text{4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47}$
 $\text{15919023B16BC3C6C46A92BBD326AADF}$

25 $2 \cdot 3^3 \cdot D^4 \pmod n = \text{FB2D57796039DFC4AF9199CAD44B66F257A1FF}$
 $\text{3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A}$
 $\text{107E45C51FCDB7462D03A35002D29823A2BB5}$

$2^2 \cdot 3^6 \cdot D^8 \pmod n = \text{4C210F96FF6C77541910623B1E49533206DFB9E91}$
 $\text{6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D}$
 $\text{82ACB23DAF1A0D5A721A1890D03A00BD8}$

30 $2^2 \cdot 3^7 \cdot D^8 \pmod n = \text{E4632EC4FE4565FC4B3126B15ADBF996149F2D}$
 $\text{BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249}$
 $\text{B1B18880616B90D4E280F564E49B270AE02388}$

35 $2^4 \cdot 3^{14} \cdot D^{16} \pmod n = \text{ED3DDC716AE3D1EA74C5AF935DE814BCC}$

2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF

665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^5 \cdot 3^{14} \cdot D^{16} \pmod n = \text{DA7C64E0E8EDBE9CF823B71AB13F17E1161487}$

6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5

5 7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} \cdot 3^{28} \cdot D^{32} \pmod n = \text{6ED6AFC5A87D2DD117B0D89072C99FB9DC9}$

5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D

722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} \cdot 3^{28} \cdot D^{32} \pmod n = \text{DDAD5F8B50FA5BA22F61B120E5933F73B92}$

10 BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8

7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} \cdot 3^{56} \cdot D^{64} \pmod n = \text{A466D0CB17614EFD961000BD9EABF4F021}$

36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA

8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

15 $2^{44} \cdot 3^{112} \cdot D^{128} \pmod n = \text{925B0EDF5047EFEC5AFABDC03A830919761}$

B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F

8FDEC740778BDC178AD7AF2968689B930D5A2359

$2^{44} \cdot 3^{113} \cdot D^{128} \pmod n = \text{B711D89C03FDEA8D1F889134A4F809B3F2D}$

8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803

20 BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} \cdot 3^{226} \cdot D^{256} \pmod n = \text{41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C}$

08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D

FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} \cdot 3^{452} \cdot D^{512} \pmod n$, that is $4^{88} \cdot 9^{226} \cdot D^{512} \pmod n = \text{28AA7F12259BFBA8}$

25 1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D

AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA

4A529

We find the commitment R . The authentication is successful.

Digital signature

30 The digital signing mechanism enables an entity called a **signing entity** to produce signed messages and an entity called a **controller** to ascertain signed messages. The message M is any binary sequence: it may be empty. The message M is signed by adding a signature appendix to it. This signature appendix comprises one or more commitments and/or challenges as well as the corresponding responses.

The controller has the same hashing function, the parameters k and m and the module n . The parameters k and m provide information to the controller. Firstly, each elementary challenge from d_1 to d_m must take a value from 0 to $2^{k-1}-1$ (the values of $v/2$ to $v-1$ are not used). Secondly, each challenge d must comprise m elementary challenges referenced from d_1 to d_m , namely as many of them as base numbers. Furthermore, failing indications to the contrary, the m base numbers from g_1 to g_m are the m first prime numbers. With $(k-1).m$ equal to 15 to 20, it is possible to sign with four GQ2 triplets produced in parallel; with $(k-1).m$ equal to 60 or more, it is possible to sign with a single GQ2 triplet. For example, with $k = 9$ and $m = 8$, a single GQ2 triplet is enough; each challenge has eight bytes and the base numbers are 2, 3, 5, 7, 11, 13, 17 and 19.

The signing operation is a sequence of three acts: an act of commitment, an act of challenge and an act of response. Each act produces one or more GQ2 triplets each comprising: a commitment R ($\neq 0$), a challenge d consisting of m elementary challenges referenced d_1, d_2, \dots, d_m and a response D ($\neq 0$).

The signing entity has a hashing function, the parameter k and the GQ2 private key, namely the factorization of the modulus n according to one of the three representations referred to here above. **Within the signing entity, it is possible to isolate a witness that performs the acts of commitment and response**, so as to isolate the functions and parameters most sensitive to the demonstrator. To compute commitments and responses, the witness has the parameter k and the GQ2 private key, namely the factorization of the modulus n according to one of the three representations referred to here above. The witness thus isolated is similar to the witness defined within the demonstrator. It may correspond to a particular embodiment, for example, • a chip card connected to a PC together forming the signing entity, or again, • programs particularly protected within a PC, or again, • programs particularly protected within a chip card.

1) The act of commitment comprises the following operations:

When the witness has m private values from Q_1 to Q_m and the modulus n , it randomly and privately draws one or more random values r ($0 < r < n$); then, by k successful squaring (mod n) operations, it converts each random value r into a commitment R .

$$R_i \equiv r^v \pmod{n}$$

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij} , it privately and randomly draws one or more collections of f random

values: each collection has one random value r_i per prime factor p_i ($0 < r_i < p_i$); then, by k successive squaring (mod p_i) operations, it converts each random value r_i into a component of commitment R_i .

$$R_i \equiv r_i^v \pmod{p_i}$$

5 For each collection of f commitment components, the witness sets up a commitment according to the Chinese remainder technique. There are as many commitments as there are collections of random values.

$$R = \text{Chinese reminders } (R_1, R_2, \dots, R_f)$$

10 **2) The act of challenge** consists in hashing all the commitments R and the message to be signed M to obtain a hashing code from which the signing entity forms one or more challenges each comprising m elementary challenges; each elementary challenge takes a value from 0 to $v/2-1$; for example with $k = 9$ and $m = 8$. Each challenge has eight bytes. There are as many challenges as there are commitments.

$$d = d_1, d_2, \dots, d_m, \text{ extracted from the result Hash}(M, R)$$

15 **3) The act of response** comprises the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n , it computes one or more responses D using each random value r of the act of commitment and the private values according to the elementary challenges.

$$X \equiv Q_1^{d_1} \cdot Q_2^{d_2} \dots Q_m^{d_m} \pmod{n}$$

$$20 \quad D \equiv r \cdot X \pmod{n}$$

When the witness has f prime factors from p_1 to p_f and $m \cdot f$ private components Q_{ij} , it computes one or more collections of f response components in using each collection of random values of the act of commitment: each collection of response components comprises one component per prime factor.

$$25 \quad X_i \equiv Q_{1,i}^{d_1} \cdot Q_{2,i}^{d_2} \dots Q_{m,i}^{d_m} \pmod{p_i}$$

$$D_i \equiv r_i \cdot X_i \pmod{p_i}$$

For each collection of response components, the witness sets up a response according to the Chinese remainders technique. There are as many responses as there are challenges.

$$30 \quad D = \text{Chinese remainders } (D_1, D_2, \dots, D_f)$$

The signing entity signs the message M in adding to it a signature appendix comprising:

- either each GQ2 triplet, namely each commitment R , each challenge d and each response D ,

- or else each commitment R and each corresponding response D ,
- or else each challenge d and each corresponding response D .

The running of the verification operation depends on the contents of the signature appendix. There are three possible cases.

Should the appendix comprise one or more triplets, the checking operation has two independent processes for which the chronology is immaterial. The controller accepts the signed message if and only if the two following conditions are fulfilled.

Firstly, each triplet must be consistent (an appropriate relationship for the following type has to be verified) and acceptable (the comparison has to be done on a non-zero value).

$$R \cdot \prod_{i=1}^m G_i^{d_i} \equiv D^{2^k} \pmod{n} \quad \text{or else} \quad R \equiv D^{2^k} \cdot \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

For example, the response D is converted by a sequence of elementary operations: k squared (mod n) separated by $k-1$ multiplication or division operations (mod n) by base numbers. For the i -th multiplication or division which is performed between the i -th square and the $i+1$ st square, the i -th bit of the elementary challenge d_1 indicates whether it is necessary to use g_1 , the i -th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2 , ... up to the i -th bit of the elementary challenge d_m which indicates if it is necessary to use g_m . It is thus necessary to retrieve each commitment R present in the signature appendix.

Furthermore, the triplet or triplets must be linked to the message M . By hashing all the commitments R and the message M , a hashing code is obtained from which each challenge d must be recovered.

$$d = d_1, d_2, \dots, d_m, \text{ identical to those extracted from the result Hash}(M, R)$$

If the appendix has no challenge, the checking operation starts with the reconstitution of one or more challenges d' by hashing all the commitments R and the message M .

$$d = d'_1, d'_2, \dots, d'_m, \text{ extracted from the result Hash}(M, R)$$

Then, the controller accepts the signed message if and only if each triplet is consistent (an appropriate relationship of the following type is verified) and acceptable (the comparison is done on a non-zero value).

$$R \cdot \prod_{i=1}^m G_i^{d'_i} \equiv D^{2^k} \pmod{n} \quad \text{or else} \quad R \equiv D^{2^k} \cdot \prod_{i=1}^m G_i^{d'_i} \pmod{n}$$

Should the appendix comprise no commitment, the checking operation starts with the reconstitution of one or more commitments R' according to one of the following two formulae, namely the one that is appropriate. No re-established commitment should be zero.

$$5 \quad R' \equiv D^{2^k} / \prod_{i=1}^m G_i^{d_i} \pmod{n} \quad \text{or else} \quad R' \equiv D^{2^k} \cdot \prod_{i=1}^m G_i^{d_i} \pmod{n}$$

Then, the controller must hash all the commitments R' and the message M so as to reconstitute each challenge d .

$d = d_1, d_2, \dots, d_m$, identical to those extracted from the result $\text{Hash}(M, R')$

10 The controller accepts the signed message if and only if each reconstituted challenge is identical to the corresponding challenge in the appendix.

In the present application, it has been shown that there are pairs of private values and public values Q and G used to implement the method, system and device according to the invention, designed to prove the authenticity of an entity and/or the integrity and/or the authenticity of a message.

15 In the pending application filed on the same day as the present application by France Télécom, TDF and the firm Math RiZK, whose inventors are Louis Guillou and Jean-Jacques Quisquater, a method has been described for the production of sets of GQ2 keys namely moduli n and pairs of public and private values G and Q when the exponent v is equal to 2^k . This patent application is incorporated herein by
20 reference.

CLAIMS

1. Method designed to prove to a controller entity,

- the authenticity of an entity and/or

5 - the integrity of a message **M** associated with this entity,

by means of:

- **m** pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m (**m** being greater than or equal to 1),

10 - a public modulus **n** constituted by the product of **f** prime factors p_1, p_2, \dots, p_f , **f** being greater than or equal to 2;

said modulus and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n};$$

v designating a public exponent;

15 said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) of the private values Q_i and of the public exponent **v**;

20 - the witness computes commitments **R** in the ring of integers modulo **n**; each commitment being computed by performing operations of the type

$$R_i \equiv r_i^v \pmod{p_i}$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots, r_f\}$, then by applying the Chinese remainder method,

25 - the witness receives one or more challenges **d**; each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D** by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \pmod{p_i}$$

then by applying the Chinese remainders method;

30 the method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R**, **d**, **D** forming a triplet referenced $\{R, d, D\}$.

35 2. Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment R by applying the process specified according to claim 1,

5 - the demonstrator sends the controller all or part of each commitment R,

• **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment R, produces challenges d whose number is equal to the number of commitments R and sends the challenges d to the demonstrator,

10 • **Step 3: act of response D**

- the witness computes the responses D from the challenges d by applying the process specified according to claim 1,

• **Step 4: act of checking**

- the demonstrator sends each response D to the controller,

15 **case where the demonstrator has transmitted a part of each commitment R**

if the demonstrator has transmitted a part of each commitment R, the controller, having the m public values G_1, G_2, \dots, G_m , computes a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type

20
$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

the controller ascertains that each reconstructed commitment R' reproduces all or part of each commitment R that has been transmitted to it,

25 **case where the demonstrator has transmitted the totality of each commitment R**

if the demonstrator has transmitted the totality of each commitment R, the controller, having the m public values G_1, G_2, \dots, G_m , ascertains that each commitment R satisfies a relationship of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

30 or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

3. Method according to claim 1, designed to provide proof to an entity, known as the controller entity, of the integrity of a message M associated with an entity called a demonstrator entity, said demonstrator entity comprising the witness;
35 said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment R by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- 5 - the demonstrator applies a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,
 - the demonstrator sends the token **T** to the controller,
 - the controller, after having received a token **T**, produces challenges **d** equal in number to the number of commitments **R** and sends the challenges **d** to the
 10 demonstrator,

• **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

- 15 - the demonstrator sends each response **D** to the controller,
 - the controller, having the **m** public values **G₁, G₂, ..., G_m**, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

20 or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

- then the controller applies the hashing function **h** whose arguments are the message **M** and all or part of each reconstructed commitment **R'** to reconstruct the token **T'**,
 - then the controller ascertains that the token **T'** is identical to the token **T**
 25 transmitted.

4. Method according to claim 1, designed to produce the digital signature of a message **M** by an entity known as the signing entity, said signing entity comprising the witness;

said signing entity executes a signing operation in order to obtain a signed message
 30 comprising:

- the message **M**,
 - the challenges **d** and/or the commitments **R**,
 - the responses **D**;

said signing entity executes the signing operation by implementing the following
 35 steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment R by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- 5 - the signing entity applies a hashing function **h** whose arguments are the message **M** and each commitment **R** to obtain a binary train,
 - from this binary train, the signing entity extracts challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

- 10 - the witness computes the responses **D** from the challenges **d** by applying the process specified according to claim 1.

5. Method according to claim 4, designed to prove the authenticity of the message **M** by checking the signed message through an entity called a controller;

- said controller entity having the signed message executes a checking operation by proceeding as follows:

• **case where the controller has commitments R, challenges d, responses D**

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the controller ascertains that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

20
$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

• • the controller ascertains that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

25
$$d = h(M, R)$$

• **case where the controller has challenges d and responses D**

if the controller has challenges **d** and responses **D**,

• • the controller reconstructs, on the basis of each challenge **d** and each response **D**, commitments **R'** satisfying relationships of the type

30
$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or relationships of the type:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

• • the controller ascertains that the message **M** and the challenges **d** satisfy the hashing function:

35
$$d = h(M, R')$$

• case where the controller has commitments **R** and responses **D**

if the controller has commitments **R** and responses **D**,

- the controller applies the hashing function and reconstructs **d'**

$$d' = h(M, R)$$

- the controller device ascertains that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1 d'^1 \cdot G_2 d'^2 \cdot \dots \cdot G_m d'^m \cdot D^v \text{ mod } n$$

or relationships of the type:

$$R \equiv D^v / G_1 d'^1 \cdot G_2 d'^2 \cdot \dots \cdot G_m d'^m \cdot \text{ mod } n$$

6. Method according to any of the claims 1 to 5, such that the components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,f}$ of the private values Q_i are numbers drawn at random at a rate of one component $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) for each of said prime factors p_j , said private values Q_i being possibly computed from said components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,f}$ by the Chinese remainder method

- 15 said public values G_i , being computed

- by performing operations of the following type:

$$G_{i,j} \equiv Q_{i,j}^v \text{ mod } p_j$$

- then by applying the Chinese remainder method to establish G_i such that

$$G_i \cdot Q_i^v \equiv 1 \cdot \text{ mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n ;$$

- 20 7. Method according to claim 6, such that the public verification exponent v is a prime number.

8. Method according to any of the claims 1 to 5, said exponent v being such that

$$v = 2^k$$

- 25 where k is a security parameter greater than 1;
said public value G_i is the square g_i^2 of the base number g_i smaller than the f prime factors p_1, p_2, \dots, p_f ; the base number g_i being such that the following conditions are met:

none of the two equations:

$$x^2 \equiv g_i \text{ mod } n \text{ and } x^2 \equiv -g_i \text{ mod } n$$

can be resolved in x in the ring of integers modulo n

and such that the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo n .

9. System designed to prove, to a controller server,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

5 by means

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m , m being greater than or equal to 1,

- a public modulus n constituted by the product of said f prime factors p_1, p_2, \dots, p_f , f being greater than or equal to 2;

10 said modulus and said values being linked by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

v designating a public exponent;

said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

15 the witness device comprises a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or $f \cdot m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) of the private values Q_i and of the public exponent v ;

said witness device also comprises:

20 - random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of integers modulo n ; each commitment being computed by performing operations of the type:

$$R_i \equiv r_i^v \pmod{p_i}$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots, r_f\}$, then by applying the Chinese remainder method;

30 said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d ; each challenge d comprising m integers d_i hereinafter called elementary challenges;

35 - computation means, hereinafter called means for the computation of the responses D of the witness device for the computation, on the basis of each challenge

d, of a response **D**, by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d_1} \cdot Q_{i,2}^{d_2} \cdot \dots \cdot Q_{i,m}^{d_m} \bmod p_i$$

and then by applying the Chinese remainder method.

5 - transmission means to transmit one or more commitments **R** and one or more responses **D**;

there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R**, **d**, **D** forming a triplet referenced **{R, d, D}**.

10 10. System according to claim 9, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller, said system being such that it comprises:

15 - a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

20 said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 9,

25 - the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

- the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator device, to transmit all or part of each commitment **R** to the controller device through the connection means;

30 • **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**,

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges d to the demonstrator,

• **Step 3: act of response D**

5 the means of reception of the challenges d of the witness device receive each challenge d coming from the demonstrator device through the interconnection means,

the means of computation of the responses D of the witness device compute the responses D from the challenges d by applying the process specified according to claim 9,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response D to the controller,

the controller device also comprises:

15 - computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R

20 if the transmission means of the demonstrator have transmitted a part of each commitment R , the computation means of the controller device, having m public values G_1, G_2, \dots, G_m , compute a reconstructed commitment R' , from each challenge d and each response D , this reconstructed commitment R' satisfying a relationship of the type

$$25 \quad R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod{n}$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod{n}$$

the comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received,

30 **case where the demonstrator has transmitted the totality of each commitment R**

if the transmission means of the demonstrator have transmitted the totality of each commitment R , the computation means and the comparison means of the controller device, having m public values G_1, G_2, \dots, G_m , ascertain that each commitment R satisfies a relationship of the type:

35

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

11. System according to claim 9, designed to give proof to an entity, known
 5 as a controller, of the integrity of a message **M** associated with an entity known as a
 demonstrator,
 said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said
 demonstrator device being interconnected with the witness device by interconnection
 10 means and possibly taking the form especially of logic microcircuits in a nomad
 object, for example the form of a microprocessor in a microprocessor-based bank
 card,

- a controller device associated with the controller entity, said controller
 device especially taking the form of a terminal or remote server; said controller
 15 device comprising connection means for its electrical, electromagnetic, optical or
 acoustic connection, especially through a data-processing communications network,
 to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

20 at each call, the means of computation of the commitments **R** of the witness device
 compute each commitment **R** by applying the process specified according to claim 9,
 - the witness device has transmission means, hereinafter called the transmission
 means of the witness device, to transmit all or part of each commitment **R** to the
 demonstrator device, through the interconnection means,

25 • **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the
 computation means of the demonstrator, applying a hashing function **h** whose
 arguments are the message **M** and all or part of each commitment **R** to compute at
 least one token **T**,

30 the demonstrator device also has transmission means, hereinafter known as the
 transmission means of the demonstrator device, to transmit each token **T** through the
 connection means to the controller device,

the controller device also has challenge production means for the production, after
 having received the token **T**, of the challenges **d** in a number equal to the number of
 35 commitments **R**,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Step 3: act of response D**

5 the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 9,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values **G₁, G₂, ..., G_m**, in order to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

20 or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the token **T'** with the received token **T**.

12. System according to claim 9, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

30 the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by

interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

5 • **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 9, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

10 • **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

15 • **Step 3: act of response D**

the means for the reception of the challenges **d**, receive each challenge **d** coming from the signing device through the interconnection means,

20 the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 9,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

25 13. System according to claim 11, designed to prove the authenticity of the message **M** by checking the signed message by means of an entity called the controller;

said system being such that it comprises a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;

30 said signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the

transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device.

• **case where the controller device has commitments **R**, challenges **d**, responses **D****
if the controller has commitments **R**, challenges **d**, responses **D**,

- • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d = h(M, R)$$

• **case where the controller device has challenges **d** and responses **D****
if the controller device has challenges **d** and responses **D**,

- • the computation means of the controller, on the basis of each challenge **d** and each response **D**, compute commitments **R'** satisfying relationships of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or relationships of the type:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{ mod } n$$

- • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

$$d = h(M, R')$$

• **case where the controller device has commitments **R** and responses **D****
if the controller device has commitments **R** and responses **D**,

• • the computation means of the controller device apply the hashing function and compute d' such that

$$d' = h(M, R)$$

• • the computation and comparison means of the controller device ascertain that the commitments R , the challenges d' and the responses D satisfy relationships of the type

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \pmod{n}$$

or relationships of the type:

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \pmod{n}$$

14. System according to any of the claims 9 to 13, such that the components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,f}$ of the private values Q_i are numbers drawn at random at a rate of one component $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) for each of said prime factors p_j , said private values Q_i being possibly computed from said components $Q_{i,1}, Q_{i,2}, \dots, Q_{i,f}$ by the Chinese remainder method

said public values G_i , being computed

• by performing operations of the following type:

$$G_{i,j} \equiv Q_{i,j}^v \pmod{p_j}$$

• then by applying the Chinese remainder method to establish G_i such that

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n};$$

15. Method according to claim 14, such that the public verification component v is a prime number.

16. Method according to any of the claims 9 to 13, said exponent v being such that

$$v = 2^k$$

where k is a security parameter greater than 1; said public value G_i being the square g_i^2 of the base number g_i smaller than the f prime factors p_1, p_2, \dots, p_f ; the base number g_i being such that the following conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \pmod{n} \text{ and } x^2 \equiv -g_i \pmod{n}$$

can be resolved in x in the ring of integers modulo n

and such that the equation:

$$x^v \equiv g_i^2 \pmod{n}$$

can be resolved in x in the ring of the integers modulo n .

17. Terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller server:

- 5 - the authenticity of an entity and/or
- the integrity of a message M associated with this entity;

by means of:

- m pairs of private values Q_1, Q_2, \dots, Q_m and public values G_1, G_2, \dots, G_m , m being greater than or equal to 1,
- 10 - a public modulus n constituted by the product of said f prime factors p_1, p_2, \dots, p_f , f being greater than or equal to 2;

said modulus and said values being related by relations of the type :

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n}.$$

v designating a public exponent;

- 15 said terminal device comprises a witness device comprising a memory zone containing the f prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or $f \cdot m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \pmod{p_j}$) of the private values Q_i and of the public exponent v ;

- 20 said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of the integers modulo n ; each commitment being computed by performing operations of the type:
- 25

$$R_i \equiv r_i^v \pmod{p_i}$$

- where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots, r_f\}$ produced by the random value production means, then by applying the Chinese remainder method;
- 30 the witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d ; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- 35 - computation means, hereinafter called means for the computation of the

responses **D** of the witness device, for the computation, on the basis of each challenge **d**, of a response **D**, by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d^1} \cdot Q_{i,2}^{d^2} \cdot \dots \cdot Q_{i,m}^{d^m} \bmod p_i$$

and then by applying the Chinese remainder method;

5 - transmission means to transmit one or more commitments **R** and one or more responses **D**;

there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R**, **d**, **D** forming a triplet referenced **{R, d, D}**.

10 18. Terminal device according to claim 17, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a
15 microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote
20 server;

said terminal device enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim
25 17,

- the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,
the demonstrator device also has transmission means, hereinafter called the
30 transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

• **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means

between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device, the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 17,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

19. Terminal device according to claim 17, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 17;

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Steps 2 and 3: act of challenge d, act of response D**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T**, through the connection means, to the controller device,

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device, through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 17,

10 • **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

20. Terminal device according to claim 17, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

20 said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

25 said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

30 said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 17, the witness device has means of transmission, hereinafter called the transmission

means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive the challenges **d** coming from the signing device through the interconnection means, the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 9,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

21. Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity.

by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values **Q₁, Q₂, ... Q_m** and public values **G₁, G₂, ... G_m**, **m** being greater than or equal to 1,

- a public modulus **n** constituted by the product of **f** prime factors **p₁, p₂, ... p_f**, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \pmod{n} \text{ or } G_i \equiv Q_i^v \pmod{n} .$$

v designating a public exponent;

Q_i designating a private value, unknown to the controller device, associated with the public value **G_i**.

22. Controller device according to claim 21, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

5 said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity;

said controller device being used to execute the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

10 said controller device also has means for the reception of all or part of the commitments **R** coming from the demonstrator device through the connection means, the controller device has challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers **d_i** hereinafter called elementary challenges.

15 the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Steps 3 and 4: act of response, act of checking**

the controller device also comprises:

- 20 - means for the reception of the responses **D** coming from the demonstrator device, through the connection means,
- computation means, hereinafter called the computation means of the controller device,
- 25 - comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the reception means of the demonstrator have received a part of each commitment **R**, the computation means of the controller device, having **m** public values **G₁, G₂, ..., G_m**, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R}' \equiv \mathbf{G}_1 \mathbf{d}_1 \cdot \mathbf{G}_2 \mathbf{d}_2 \cdot \dots \mathbf{G}_m \mathbf{d}_m \cdot \mathbf{D}^v \bmod n$$

or a relationship of the type

$$\mathbf{R}' \equiv \mathbf{D}^v / \mathbf{G}_1 \mathbf{d}_1 \cdot \mathbf{G}_2 \mathbf{d}_2 \cdot \dots \mathbf{G}_m \mathbf{d}_m \cdot \bmod n$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

35

case where the demonstrator has transmitted the totality of each commitment **R**

if the reception means of the demonstrator have received the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values **G₁, G₂, ..., G_m**, ascertain that each commitment **R** satisfies a relationship of the type:

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \text{ mod } n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n$$

23. Controller device according to claim 21, designed to prove the integrity of a message **M** associated with an entity known as a demonstrator, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity,

said controller device enabling the execution of the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

said controller device also has means for the reception of tokens **T** coming from the demonstrator device through the connection means,

the controller device has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers, hereinafter called elementary challenges,

the controller device also has transmission means, hereinafter called the transmission means of the controller device, to transmit the challenges **d** to the demonstrator through the connection means;

• **Steps 3 and 4: act of response D, act of checking**

the controller device also comprises:

- means for the reception of the responses **D** coming from the demonstrator device, through the connection means,

the controller device also comprises

- computation means, hereinafter called the computation means of the controller device, having **m** public values **G₁, G₂, ..., G_m**, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n$$

then, secondly, compute a token T' by applying the hashing function h having as arguments the message M and all or part of each reconstructed commitment R' ,
 5 the controller device also comprises comparison means, hereinafter called the comparison means of the controller device, to compare the token T' with the received token T .

24. Controller device according to claim 21, designed to prove the authenticity of the message M by checking a signed message by means of an entity
 10 called a controller;

the signed message, sent by a signing device associated with a signing entity having a hashing function $h(M, R)$, comprising:

- the message M ,
- 15 - the challenges d and/or the commitments R ,
- the response D ;

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity,

20 said controller device having received the signed message from the signing device, through the connection means,

the controller device comprises:

- computation means, hereinafter called the computation means of the controller device,

- 25 - comparison means, hereinafter called the comparison means of the controller device;

- case where the controller device has commitments R , challenges d , responses D if the controller has commitments R , challenges d , responses D ,

- • the computation and comparison means of the controller device ascertain
 30 that the commitments R , the challenges d and the responses D satisfy relationships of the type:

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot \bmod n$$

• • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function

$$d = h(M, R)$$

5 • case where the controller device has challenges **d** and responses **D**

if the controller device has challenges **d** and responses **D**,

• • the computation means of the controller device, on the basis of each challenge **d** and each response **D**, compute commitments **R'** satisfying relationships of the type

10
$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \pmod n$$

or relationships of the type:

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \pmod n$$

• • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

15
$$d = h(M, R')$$

• case where the controller device has commitments **R** and responses **D**

if the controller device has commitments **R** and responses **D**,

• • the computation means of the controller device apply the hashing function and compute **d'** such that

20
$$d' = h(M, R)$$

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot D^v \pmod n$$

25 or relationships of the type:

$$R \equiv D^v / G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \pmod n$$