CLAIMS

1. A position information authentication system (~~1~~) comprising:

a positioning terminal (~~200~~) that receives a navigation message, and when the navigation message that has been received corresponds to a navigation message to be authenticated, wirelessly transmits position information indicating a present position outside, the present position being computed by using the navigation message;

an authentication center apparatus (~~100~~) that transmits a center-generated authentication data to a communication satellite (~~3~~) transmitting the center-generated authentication data used by the positioning terminal (~~200~~) for authentication; and

a position information acquisition apparatus (~~300, 300A~~) that receives the position information, which is wirelessly transmitted by the positioning terminal (~~200~~),

wherein

the authentication center apparatus (~~100~~) includes:

a center-side satellite reception portion (~~110~~) that receives from a navigation satellite (~~2~~) included in a navigation satellite system, a satellite electric wave including the navigation message;

a center-side authentication data generation portion (~~122~~) that generates a cryptography key, and generates the center-generated authentication data based on the cryptography key and the navigation message, which is included in the satellite electric wave received by the center-side satellite reception portion (~~110~~); and

an authentication data transmission portion (~~130~~) that transmits the center-generated authentication data, which is generated by the center-side authentication data generation portion (~~122~~), to the communication satellite (~~3~~),

the positioning terminal (~~200~~) includes:

a terminal-side satellite reception portion (~~230~~) that receives the center-generated authentication data from the communication satellite (~~3~~), and receives the satellite electric wave from the navigation satellite (~~2~~);

a key reception portion (~~211~~) that receives a key-related data from the authentication center apparatus (~~100~~), the key-related data being one of the cryptography key and a key generation data capable of generating the cryptography key;

a terminal-side authentication data generation portion (~~S54~~) that generates a terminal-generated authentication data based on the key-related data, which is received by the key reception portion (~~211~~), and the navigation message, which is extracted from the satellite electric wave received by the terminal-side satellite reception portion (~~230~~);

an authentication determination portion (~~S56 through S60~~) that compares the center-generated authentication data with the terminal-generated authentication data and, when the center-generated authentication data and the terminal-generated authentication data are matched, determines that the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion (~~230~~) is authenticated;

an authenticated data generation portion (~~S6 through S10~~) that generates an authenticated data indicating the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion (~~230~~) is authenticated, based on the key-related data received by the key reception portion (~~211~~) from the authentication center apparatus (~~100~~); and

a terminal-side transmission portion (~~212~~) that transmits the position information computed based on the navigation message and the authenticated data, which is generated by the authenticated data generation portion (~~S6 through S10~~), and

the position information acquisition apparatus (~~300, 300A~~) includes:

a terminal data acquisition portion (~~S70, S112~~) that acquires the position information and the authenticated data transmitted by the terminal-side transmission portion (~~212~~) from a communication portion;

a key acquisition portion (~~S74, S96~~) that acquires the key-related data from the authentication center apparatus (~~100~~) through the communication portion;

a comparative data generation portion ~~(S78, S100, S102)~~ that, based on the key-related data acquired by the key acquisition portion ~~(S74, S96)~~, generates an authenticated comparative data to be compared with the authenticated data; and

a terminal determination portion ~~(S80 through S84, S114 through S120)~~ that compares the authenticated data, which is acquired by the terminal data acquisition portion ~~(S70, S112)~~, with the authenticated comparative data, which is generated by the comparative data generation portion ~~(S78, S100, S102)~~ and, when the authenticated data acquired by the terminal data acquisition portion ~~(S70, S112)~~ is matched with the authenticated comparative data generated by the comparative data generation portion ~~(S78, S100, S102)~~, determines that the positioning terminal ~~(200)~~ corresponds to a regular positioning terminal.

2. The position information authentication system according to claim 1, wherein:

the authenticated data generation portion ~~(S6 through S10)~~ generates the authenticated data by a hash function using the key-related data received by the key reception portion ~~(211)~~.

3. The position information authentication system according to claim 2, wherein:

the authenticated data generation portion ~~(S6 through S10)~~ generates the authenticated data by the hash function using the terminal-generated authentication data along with the key-related data received by the key reception portion ~~(211)~~.

4. The position information authentication system according to any one of claims 1-3, wherein:

the position information acquisition apparatus ~~(300A)~~ includes

an acquirer-side satellite reception portion ~~(330)~~ that receives the satellite electric wave from the navigation satellite ~~(2)~~,

an electric wave information extraction portion ~~(S92)~~ that extracts a satellite number and time information from the satellite electric wave received by the acquirer-side satellite reception portion, and

an electric wave information transmission portion ~~(S94)~~ that allows the communication portion to periodically transmit the satellite number and the time information extracted by the electric wave information extraction portion to the authentication center apparatus;

the key acquisition portion ~~(S96)~~ acquires the key-related data transmitted from the authentication center apparatus based on transmission of the satellite number and the time information from the communication portion to the authentication center apparatus from the communication portion;

the comparative data generation portion ~~(S100, S102)~~ generates the authenticated comparative data, and determines in advance a correspondence relation among the authenticated comparative data, the satellite number, and the time information before receiving the authenticated data; and

when the authenticated comparative data determined by the correspondence relation, the satellite number, and the time information acquired by the terminal data acquisition portion ~~(S70, S112)~~ exists, the terminal determination portion ~~(S114 through S120)~~ compares the authenticated comparative data with the authenticated data acquired by the terminal data acquisition portion ~~(S70, S112)~~.

5. A positioning terminal ~~(200)~~ that receives a navigation message and, when the navigation message that has been received corresponds to a navigation message to be authenticated, wirelessly transmits position information indicating a present position outside, the present position being computed by using the navigation message, the positioning terminal ~~(200)~~ comprising:

a terminal-side satellite reception portion ~~(230)~~ that receives a center-generated authentication data from a communication satellite ~~(3)~~, the

center-generated authentication data being generated by an authentication center apparatus ~~(100)~~ and transmitted to the communication satellite ~~(3)~~ to

be used for authentication in the positioning terminal ~~(200)~~, and receives a satellite electric wave including the navigation message from a navigation satellite ~~(2)~~ included in a navigation satellite system;

a key reception portion ~~(211)~~ that receives a key-related data from the authentication center apparatus ~~(100)~~, the key-related data being one of a cryptography key to generate the center-generated authentication data and a key generation data capable of generating the cryptography key;

a terminal-side authentication data generation portion ~~(S54)~~ that generates a terminal-generated authentication data based on the key-related data received by the key reception portion ~~(211)~~ and the navigation message extracted from the satellite electric wave received by the terminal-side satellite reception portion ~~(230)~~;

an authentication determination portion ~~(S56 through S60)~~ that compares the center-generated authentication data with the terminal-generated authentication data and, when the center-generated authentication data is matched with the terminal-generated authentication data, determines the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion ~~(230)~~ is authenticated;

an authenticated data generation portion ~~(S6 through S10)~~ that generates an authenticated data indicating the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion ~~(230)~~ is authenticated, based on the key-related data received by the key reception portion ~~(211)~~ from the authentication center apparatus ~~(100)~~; and

a terminal-side transmission portion ~~(212)~~ that transmits the position information computed based on the navigation message and the authenticated data generated by the authenticated data generation portion ~~(S6 through S10)~~.

6. A position information acquisition apparatus ~~(300, 300A)~~ that receives a navigation message and, when the navigation message that has been received corresponds to a navigation message to be authenticated,

receives position information and an authenticated data from a positioning terminal ~~(200)~~ that wirelessly transmit the position information and the authenticated data outside, the position information indicating the present position computed using the navigation message, the authenticated data indicating the navigation message that has been received is authenticated, the position information acquisition apparatus ~~(300, 300A)~~ comprising:

a terminal data acquisition portion ~~(S70, S112)~~ that acquires the position information and the authenticated data transmitted by the positioning terminal ~~(200)~~ from a communication portion;

a key acquisition portion ~~(S74, S96)~~ that allows the communication portion to acquire a key-related data from an authentication center apparatus ~~(100)~~, wherein the key-related data corresponds to one of a cryptography key and a key generation data, the cryptography key being used by the authentication center apparatus ~~(100)~~ to generate a center-generated authentication data that is used by the positioning terminal ~~(200)~~ for authentication, the key generation data being capable of generating the cryptography key;

a comparative data generation portion ~~(S78, S100, S102)~~ that generates an authenticated comparative data to be compared with the authenticated data based on the key-related data acquired by the key acquisition portion ~~(S74, S96)~~; and

a terminal determination portion ~~(S80 through S84, S114 through S120)~~ that compares the authenticated data acquired by the terminal data acquisition portion ~~(S70, S112)~~ with the authenticated comparative data generated by the comparative data generation portion ~~(S78, S100, S102)~~ and, when the authenticated data acquired by the terminal data acquisition portion ~~(S70, S112)~~ is matched with the authenticated comparative data generated by the comparative data generation portion ~~(S78, S100, S102)~~, determines that the positioning terminal ~~(200)~~ is a regular positioning terminal.