CLAIMS

1. A navigation message authentication system (~~1~~), comprising:

at least one first satellite (~~2~~) that transmits a first navigation message;

a second satellite (~~3~~) that transmits a second navigation message including an inspection data used for an authentication process for the first navigation message;

a reception terminal (~~200~~) that receives the first navigation message and the second navigation message, wherein the navigation message authentication system (~~1~~) performs the authentication process of authenticating whether the first navigation message received by the reception terminal (~~200~~) is the first navigation message transmitted from the first satellite (~~2~~) by using the inspection data included in the second navigation message; and

an authentication processing apparatus (~~300~~) that is provided outside the reception terminal (~~200~~) and communicates with the reception terminal (~~200~~),

wherein:

the reception terminal (~~200~~) includes

a terminal-side satellite receiver (~~230~~) that receives the first navigation message transmitted from the first satellite (~~2~~) and the second navigation message transmitted from the second satellite (~~3~~),

an inspection data extraction section (~~S2~~) that extracts the inspection data from the second navigation message received by the terminal-side satellite receiver (~~230~~),

an authentication relation data extraction section (~~S5~~) that extracts, from the first navigation message received by the terminal-side satellite receiver (~~230~~), an authentication relation data required for the authentication process for the first navigation message,

an authentication request signal generation section (~~S7~~) that generates an authentication request signal which includes the inspection data extracted by the inspection data extraction section (~~S2~~) and the authentication relation data extracted by the authentication relation data

extraction section (~~S5~~), and requests the authentication process to be performed for the first navigation message received by the terminal-side satellite receiver (~~230~~), and

an authentication request signal transmission processing section (~~S8~~) that transmits the authentication request signal generated by the authentication request signal generation section (~~S7~~); and

the authentication processing apparatus (~~300~~) includes

an authentication request signal reception processing section (~~S11~~) that receives the authentication request signal transmitted from the authentication request signal transmission processing section (~~S8~~), and

an authentication arithmetic operation section (~~S20~~) that performs the authentication process for the first navigation message received by the reception terminal (~~200~~), based on the inspection data and the authentication relation data each included in the authentication request signal.

2. The navigation message authentication system according to claim 1, wherein:

the inspection data included in the second navigation message is generated by an authentication center apparatus (~~100~~) that acquires the first navigation message;

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

a first navigation message reception portion (~~110~~) that receives the first navigation message,

an authentication data generation portion (~~1221~~) that generates an authentication data from the authentication relation data of the first navigation message received by the first navigation message reception portion (~~110~~),

an encryption key generation portion (~~1223~~) that generates an encryption key corresponding to the authentication data generated by the authentication data generation portion (~~1221~~),

an inspection data generation portion (~~1224~~) that generates the inspection data by using the authentication data generated by the

authentication data generation portion (~~1221~~) and the encryption key corresponding to the authentication data,

a storage portion (~~124~~) that stores the encryption key generated by the encryption key generation portion (~~1223~~) in association with the authentication data using the encryption key,

an inspection data transmission portion (~~130~~) that transmits the inspection data generated by the inspection data generation portion (~~1224~~) to the second satellite (~~3~~), and

a communication portion (~~126~~) that communicates with the authentication processing apparatus (~~300~~);

the storage portion (~~124~~) stores the encryption key in association with the inspection data and the first navigation message;

the authentication processing apparatus (~~300~~) further includes

an encryption key acquisition section (~~S24 and S25~~) that acquires, from the storage portion (~~124~~), the encryption key corresponding to the authentication relation data included in the authentication request signal, and

a comparison inspection data generation section (~~S26~~) that generates a comparison inspection data from the authentication relation data included in the authentication request signal and from the encryption key acquired by the encryption key acquisition section (~~S24 and S25~~); and

the authentication arithmetic operation section (~~S20~~)

determines that the first navigation message received by the reception terminal (~~200~~) has succeeded in authentication when the comparison inspection data generated by the comparison inspection data generation section (~~S26~~) matches the inspection data included in the authentication request signal, and

determines that the first navigation message has failed in authentication when the comparison inspection data generated by the comparison inspection data generation section (~~S26~~) does not match the inspection data included in the authentication request signal.

3. The navigation message authentication system according to claim 1 or 2, wherein:

the authentication processing apparatus ~~(300)~~ further includes

an authenticated data memory portion ~~(340)~~ that stores, as an authenticated data, a combination of the authentication relation data and the inspection data, the combination being determined to have succeeded in authentication as a result of the authentication process performed by the authentication arithmetic operation section ~~(S20)~~,

an authentication completion determination section ~~(S13)~~ that determines whether the authenticated data stored in the authenticated data memory portion ~~(340)~~ includes the authenticated data corresponding to the authentication relation data included in the authentication request signal, and

an authenticated data comparison-and-authentication section ~~(S14 to S16)~~ that performs, when the authentication completion determination section ~~(S13)~~ determines that the authenticated data stored in the authenticated data memory portion ~~(340)~~ include the authenticated data corresponding to the authentication relation data included in the authentication request signal, the authentication process for the first navigation message received by the reception terminal ~~(200)~~ based on the authentication relation data and the authenticated data corresponding to the authentication relation data; and

the authentication arithmetic operation section ~~(S20)~~ performs the authentication process when the authentication completion determination section ~~(S13)~~ determines that the authenticated data stored in the authenticated data memory portion ~~(340)~~ does not include the authenticated data corresponding to the authentication relation data included in the authentication request signal.

4. The navigation message authentication system according to claim 3, further comprising:

at least one service center ~~(400, 400a, 400b)~~ that performs communication with the authentication processing apparatus ~~(300)~~ and the reception terminal ~~(200)~~,

wherein:

the service center ~~(400, 400a, 400b)~~ includes

a service-center-side authentication request signal reception processing section ~~(S51)~~ that receives the authentication request signal transmitted from the authentication request signal transmission processing section ~~(S8)~~,

a service-center-side authenticated data memory portion ~~(440)~~ that stores, as the authenticated data, the combination of the authentication relation data and the inspection data, the combination being determined to have succeeded in authentication in the authentication process performed by the authentication arithmetic operation section ~~(S20)~~, and

a service-center-side authenticated data comparison-and-authentication section ~~(S54 to S56)~~ that performs the authentication process for the first navigation message received by the reception terminal ~~(200)~~ based on the authentication relation data included in the authentication request signal and the authenticated data corresponding to the authentication relation data.

5. The navigation message authentication system according to claim 4, wherein:

the service center ~~(400, 400a, 400b)~~ further includes

a service-center-side authentication completion determination section ~~(S53)~~ that determines whether the authenticated data stored in the service-center-side authenticated data memory portion ~~(440)~~ includes the authenticated data corresponding to the authentication relation data included in the authentication request signal, and

a service-center-side authentication request signal transmission processing section ~~(S57)~~ that transmits the authentication request signal to the authentication processing apparatus ~~(300)~~ when the service-center-side authentication completion determination section ~~(S53)~~ determines that the authenticated data stored in the service-center-side authenticated data memory portion ~~(440)~~ does not include the authenticated

data corresponding to the authentication relation data included in the authentication request signal;

the authentication request signal reception processing section ~~(S11)~~ of the authentication processing apparatus ~~(300)~~ receives the authentication request signal transmitted from the service-center-side authentication request signal transmission processing section ~~(S57)~~;

either one of the authentication arithmetic operation section ~~(S20)~~ and the authenticated data comparison-and-authentication section ~~(S14 to S16)~~ of the authentication processing apparatus ~~(300)~~ performs the authentication process based on the authentication relation data and the inspection data each included in the authentication request signal;

the authentication processing apparatus ~~(300)~~ transmits an authentication result data showing a result of the authentication process to the service center ~~(400, 400a, 400b)~~; and

the service center ~~(400, 400a, 400b)~~ further includes

an authentication result acquisition section ~~(S58)~~ that acquires the authentication result data transmitted from the authentication processing apparatus ~~(300)~~, and

a service-center-side authenticated data addition processing section ~~(S60)~~ that adds, as the authenticated data, the combination of the authentication relation data and the inspection data to the service-center-side authenticated data memory portion ~~(440)~~ when a result shown by the authentication result data acquired by the authentication result acquisition section ~~(S58)~~ is successful authentication.

6. The navigation message authentication system according to claim 5, wherein:

the service center ~~(400, 400a, 400b)~~ includes

an authentication result transmission processing section ~~(S62)~~ that transmits a result of authentication requested by the authentication request signal to the reception terminal ~~(200)~~.

7. The navigation message authentication system according to any one of claims 1 to 6, wherein:

the reception terminal ~~(200)~~ includes

a reception portion ~~(211)~~ that receives a result of the authentication process requested by the authentication request signal.

8. The navigation message authentication system according to any one of claims 5 to 7, wherein:

the service center ~~(400, 400a, 400b)~~ includes

a service-center-side satellite receiver ~~(430)~~ that receives the first navigation message transmitted from the first satellite ~~(2)~~ and the second navigation message;

the service-center-side authentication request signal transmission processing section ~~(S57)~~ extracts the inspection data from the second navigation message received by the service-center-side satellite receiver, while extracting the authentication relation data from the first navigation message received by the service-center-side satellite receiver, generates the authentication request signal including the inspection data and the authentication relation data, and transmits the authentication request signal to the authentication processing apparatus ~~(300)~~.

9. The navigation message authentication system according to any one of claims 4 to 8, further comprising:

a plurality of the service centers ~~(400, 400a, 400b)~~,

wherein:

the reception terminal ~~(200)~~ includes

a transmission destination selection portion ~~(222)~~ that selects a transmission destination of the authentication request signal from among the plurality of service centers ~~(400, 400a, 400b)~~; and

the authentication request signal transmission processing section ~~(S8)~~ transmits the authentication request signal to the service center ~~(400, 400a, 400b)~~ selected by the transmission destination selection portion.

10. The navigation message authentication system according to any one of claims 4 to 8, wherein:

the reception terminal ~~(200)~~ includes

a terminal-side transmission portion ~~(212)~~ that determines a position of the reception terminal ~~(200)~~ based on a signal from the first satellite ~~(2)~~ and also transmits position information showing a result of positioning to the service center ~~(400, 400a, 400b)~~; and

the service center ~~(400, 400a, 400b)~~ includes

a service-center-side reception portion ~~(411)~~ that receives the position information transmitted from the reception terminal ~~(200)~~, and implements a service using the position information received by the service-center-side reception portion ~~(411)~~.

11. The navigation message authentication system according to any one of claims 1 to 10, wherein:

the authentication relation data includes information for specifying a transmitter of the first navigation message, which is intrinsic to the transmitter, and transmission time information for specifying a transmission time of the first navigation message.

12. A reception terminal, comprising:

a terminal-side satellite receiver ~~(230)~~ that receives

a first navigation message transmitted from a first satellite ~~(2)~~ and

a second navigation message transmitted from a second satellite ~~(3)~~ and including inspection data used for an authentication process for the first navigation message;

an inspection data extraction section ~~(S2)~~ that extracts the inspection data from the second navigation message received by the terminal-side satellite receiver ~~(230)~~;

an authentication relation data extraction section ~~(S5)~~ that extracts, from the first navigation message received by the terminal-side satellite

receiver ~~(230)~~, an authentication relation data as a portion required for the authentication process for the first navigation message;

an authentication request signal generation section ~~(S7)~~ that generates an authentication request signal which includes the inspection data extracted by the inspection data extraction section ~~(S2)~~ and the authentication relation data extracted by the authentication relation data extraction section ~~(S5)~~ and requests the authentication process for the first navigation message received by the terminal-side satellite receiver ~~(230)~~ to be performed; and

an authentication request signal transmission processing section (S8) that transmits the authentication request signal generated by the authentication request signal generation section ~~(S7)~~.

13. An authentication processing apparatus, comprising:

an authentication request signal reception processing section ~~(S11)~~ that receives an authentication request signal including an authentication relation data as a portion required for an authentication process for the first navigation message and inspection data used for the authentication process for the first navigation message of a first navigation message transmitted from a first satellite ~~(2)~~; and

an authentication arithmetic operation section ~~(S20)~~ that performs the authentication process for the first navigation message received by a reception terminal ~~(200)~~ based on the inspection data and the authentication relation data each included in the authentication request signal.