

C L A I M S

1. A policy management system including a user terminal, an ID provider system configured to manage an identity of a user who operates the user terminal, and a service provider system configured to provide service data to the user terminal,

the user terminal comprising:

login execution means for executing a login process with the ID provider system in accordance with an operation of the user;

first transmission means for transmitting to the ID provider system an access request message including an ID provider authentication token, which is issued at a time of the login process and includes a user ID which identifies the user, and a service provider ID which identifies the service provider system; and

reproducing means for receiving the service data which is transmitted from the service provider system, and reproducing the received service data,

the ID provider system comprising:

first storage means for storing user attribute information which includes at least the user ID and a department to which the user belongs, and in which item names and item values of attributes of the user for identifying the user are associated;

second storage means for storing a pair of an old policy and a new policy, with respect to each said service provider ID, the old policy and the new policy defining at least a determination condition for permitting transmission of the service data by the service provider system identified by the service provider ID, and a transition period indicative of a period during which a determination

result by the determination condition of not only the new policy but also the old policy is referred to when the old policy is transitioned to the new policy, the determination condition including a plurality of conditions which are  
5 identified by a determination ID, and each of the plurality of conditions including a condition indicating the department to which the user belongs, and further including a plurality of detailed conditions and a duty of registration of the user ID, a duty of transmission of an  
10 authentication federation request message, and a duty of transmission of a refusal screen information;

third storage means for storing difference-adaptive definition information with respect to each said service provider ID, the difference-adaptive definition information  
15 including a first difference determination condition which is referred to when a date of transmission of the transmitted access request message is within the transition period, the first difference determination condition indicating the determination ID of a policy having priority  
20 according to an evaluation result of the old policy and an evaluation result of the new policy, and a second difference determination condition which is referred to when the date of transmission of the transmitted access request message is out of the transition period, the second  
25 difference determination condition including a condition, which is identified by a difference-adaptive ID, and a duty of deletion of the user ID;

first acquisition means for acquiring, upon receiving the transmitted access request message, the new policy  
30 corresponding to the service provider ID in the access request message;

first determination means for determining whether the date of transmission of the access request message is

included in the transition period defined in the acquired new policy;

second acquisition means for acquiring the old policy corresponding to the acquired new policy, if a  
5 determination result by the first determination means indicates that the date of transmission is included;

confirmation means for acquiring the user attribute information stored in the first storage means, based on the user ID included in the ID provider authentication token in  
10 the access request message, and confirming whether the user ID is stored in the service provider system identified by the service provider ID in the access request message;

notification reception means for receiving a notification which is transmitted from the service provider  
15 system and corresponds to the confirmation means, the notification indicating that the user ID is stored or that the user ID is not stored;

policy evaluation means for evaluating the acquired new policy, or the acquired new policy and old policy,  
20 based on the acquired user attribute information;

second determination means for determining whether there is a need to acquire the difference-adaptive definition information, based on an evaluation result by the policy evaluation means and the notification received  
25 by the notification reception means;

third acquisition means for acquiring the difference-adaptive definition information, if a determination result by the second determination means indicates that there is the need to acquire the difference-adaptive definition  
30 information;

decision means for deciding on the determination ID that is applied, based on at least the evaluation result  
| ~~(and also by referring to the difference-adaptive~~

~~definition information when the difference adaptive definition information was acquired by the third acquisition means);~~

execution request means for requesting execution of  
5 the duty in the condition identified by the determination ID that was decided on ~~(and also requesting execution of the duty in the second difference determination condition when the second difference determination condition defined in the difference adaptive definition information was~~  
10 ~~referred to by the decision means);~~

second transmission means for transmitting, in accordance with a request from the execution request means, an authentication federation message including at least the user ID, which is included in the ID provider  
15 authentication token in the access request message, to the service provider system identified by the service provider ID in the access request message; and

third transmission means for transmitting to the user terminal, in accordance with a request from the execution  
20 request means, refusal screen information which effects display to indicate that transmission of the service data by the service provider identified by the service provider ID in the access request message was refused, and

the service provider system comprising:

25 fourth storage means for storing user attribute information in which item names and item values of attributes of the user for identifying the user, who uses service data, are associated;

issuance means for verifying, upon receiving the  
30 transmitted authentication federation request message, validity of the authentication federation request message, based on the user ID in the authentication federation request message, and issuing, if a result of the

verification indicates the validity, a service provider authentication token including the user ID used in the verification; and

5 fourth transmission means for transmitting the service data to the user terminal identified by the user ID in the issued service provider authentication token,

10 wherein the decision means decides on the determination ID that is applied also by referring to the difference-adaptive definition information when the difference-adaptive definition information was acquired by the third acquisition means, and

15 wherein the execution request means requests execution of the duty in the second difference determination condition when the second difference determination condition defined in the difference-adaptive definition information was referred to by the decision means.

2. An ID provider system which is communicable with a user terminal configured to transmit an access request message which includes an ID provider authentication token including a user ID that identifies a user, and includes a service provider ID which identifies a service provider system, and is communicable with a service provider system configured to provide service data to the user terminal and to include storage means for storing user attribute information in which item names and item values of attributes of the user for identifying the user, who uses service data, are associated, the ID provider system comprising:

30 first storage means for storing user attribute information which includes at least the user ID and a department to which the user belongs, and in which item

names and item values of attributes of the user for identifying the user are associated;

second storage means for storing a pair of an old policy and a new policy, with respect to each said service provider ID, the old policy and the new policy defining at least a determination condition for permitting transmission of the service data by the service provider system identified by the service provider ID, and a transition period indicative of a period during which a determination result by the determination condition of not only the new policy but also the old policy is referred to when the old policy is transitioned to the new policy, the determination condition including a plurality of conditions which are identified by a determination ID, and each of the plurality of conditions including a condition indicating the department to which the user belongs, and further including a plurality of detailed conditions and a duty of registration of the user ID, a duty of transmission of an authentication federation request message, and a duty of transmission of a refusal screen information;

third storage means for storing difference-adaptive definition information with respect to each said service provider ID, the difference-adaptive definition information including a first difference determination condition which is referred to when a date of transmission of the transmitted access request message is within the transition period, the first difference determination condition indicating the determination ID of a policy having priority according to an evaluation result of the old policy and an evaluation result of the new policy, and a second difference determination condition which is referred to when the date of transmission of the transmitted access request message is out of the transition period, the second

difference determination condition including a condition,  
which is identified by a difference-adaptive ID, and a duty  
of deletion of the user ID;

first acquisition means for acquiring, upon receiving  
5 the transmitted access request message, the new policy  
corresponding to the service provider ID in the access  
request message;

first determination means for determining whether the  
date of transmission of the access request message is  
10 included in the transition period defined in the acquired  
new policy;

second acquisition means for acquiring the old policy  
corresponding to the acquired new policy, if a  
determination result by the first determination means  
15 indicates that the date of transmission is included;

confirmation means for acquiring the user attribute  
information stored in the first storage means, based on the  
user ID included in the ID provider authentication token in  
the access request message, and confirming whether the user  
20 ID is stored in the service provider system identified by  
the service provider ID in the access request message;

notification reception means for receiving a  
notification which is transmitted from the service provider  
system and corresponds to the confirmation means, the  
25 notification indicating that the user ID is stored or that  
the user ID is not stored;

policy evaluation means for evaluating the acquired  
new policy, or the acquired new policy and old policy,  
based on the acquired user attribute information;

30 second determination means for determining whether  
there is a need to acquire the difference-adaptive  
definition information, based on an evaluation result by

the policy evaluation means and the notification received by the notification reception means;

third acquisition means for acquiring the difference-adaptive definition information, if a determination result  
5 by the second determination means indicates that there is the need to acquire the difference-adaptive definition information;

decision means for deciding on the determination ID that is applied, based on at least the evaluation result  
10 ~~(and also by referring to the difference adaptive definition information when the difference adaptive definition information was acquired by the third acquisition means);~~

execution request means for requesting execution of  
15 the duty in the condition identified by the determination ID that was decided on ~~(and also requesting execution of the duty in the second difference determination condition when the second difference determination condition defined in the difference adaptive definition information was~~  
20 ~~referred to by the decision means);~~

first transmission means for transmitting, in accordance with a request from the execution request means, an authentication federation message including at least the user ID, which is included in the ID provider  
25 authentication token in the access request message, to the service provider system identified by the service provider ID in the access request message; and

second transmission means for transmitting to the user terminal, in accordance with a request from the execution  
30 request means, refusal screen information which effects display to indicate that transmission of the service data by the service provider identified by the service provider ID in the access request message was refused,

wherein the decision means decides on the determination ID that is applied also by referring to the difference-adaptive definition information when the difference-adaptive definition information was acquired by the third acquisition means, and

wherein the execution request means requests execution of the duty in the second difference determination condition when the second difference determination condition defined in the difference-adaptive definition information was referred to by the decision means.

3. A policy evaluation device for use in an ID provider system which is communicable with a user terminal configured to transmit an access request message which includes an ID provider authentication token including a user ID that identifies a user, and includes a service provider ID which identifies a service provider system, and is communicable with a service provider system configured to provide service data to the user terminal and to include storage means for storing user attribute information in which item names and item values of attributes of the user for identifying the user, who uses service data, are associated, the ID provider system including:

first storage means for storing user attribute information which includes at least the user ID and a department to which the user belongs, and in which item names and item values of attributes of the user for identifying the user are associated;

second storage means for storing a pair of an old policy and a new policy, with respect to each said service provider ID, the old policy and the new policy defining at least a determination condition for permitting transmission of the service data by the service provider system

identified by the service provider ID, and a transition period indicative of a period during which a determination result by the determination condition of not only the new policy but also the old policy is referred to when the old policy is transitioned to the new policy, the determination condition including a plurality of conditions which are identified by a determination ID, and each of the plurality of conditions including a condition indicating the department to which the user belongs, and further including a plurality of detailed conditions and a duty of registration of the user ID, a duty of transmission of an authentication federation request message, and a duty of transmission of a refusal screen information; and

third storage means for storing difference-adaptive definition information with respect to each said service provider ID, the difference-adaptive definition information including a first difference determination condition which is referred to when a date of transmission of the transmitted access request message is within the transition period, the first difference determination condition indicating the determination ID of a policy having priority according to an evaluation result of the old policy and an evaluation result of the new policy, and a second difference determination condition which is referred to when the date of transmission of the transmitted access request message is out of the transition period, the second difference determination condition including a condition, which is identified by a difference-adaptive ID, and a duty of deletion of the user ID,

the policy evaluation device comprising:

first acquisition means for acquiring, upon receiving the transmitted access request message, the new policy

corresponding to the service provider ID in the access request message;

first determination means for determining whether the date of transmission of the access request message is  
5 included in the transition period defined in the acquired new policy;

second acquisition means for acquiring the old policy corresponding to the acquired new policy, if a determination result by the first determination means  
10 indicates that the date of transmission is included;

confirmation means for acquiring the user attribute information stored in the first storage means, based on the user ID included in the ID provider authentication token in the access request message, and confirming whether the user  
15 ID is stored in the service provider system identified by the service provider ID in the access request message;

notification reception means for receiving a notification which is transmitted from the service provider system and corresponds to the confirmation means, the  
20 notification indicating that the user ID is stored or that the user ID is not stored;

policy evaluation means for evaluating the acquired new policy, or the acquired new policy and old policy, based on the acquired user attribute information;

25 second determination means for determining whether there is a need to acquire the difference-adaptive definition information, based on an evaluation result by the policy evaluation means and the notification received by the notification reception means;

30 third acquisition means for acquiring the difference-adaptive definition information, if a determination result by the second determination means indicates that there is

the need to acquire the difference-adaptive definition information;

decision means for deciding on the determination ID that is applied, based on at least the evaluation result  
5 ~~(and also by referring to the difference adaptive definition information when the difference adaptive definition information was acquired by the third acquisition means); and~~

execution request means for requesting execution  
10 of the duty in the condition identified by the determination ID that was decided on ~~(and also requesting execution of the duty in the second difference determination condition when the second difference determination condition defined in the difference adaptive definition information was referred to by the decision means),~~

wherein the decision means decides on the determination ID that is applied also by referring to the difference-adaptive definition information when the  
20 difference-adaptive definition information was acquired by the third acquisition means, and

wherein the execution request means requests execution of the duty in the second difference determination condition when the second difference determination  
25 condition defined in the difference-adaptive definition information was referred to by the decision means.