

SERVICE PROCESSING METHOD AND APPARATUS

TECHNICAL FIELD

[0001] Embodiments of this specification relate to the field of data processing technologies, and in particular, to a service processing method and apparatus.

BACKGROUND

[0002] With development of Internet technologies, more services start to go online, to provide a more convenient service for a user. For an international acquiring service in the conventional technology, because a system is imperfect or a growing process is too barbaric, many prior product logic is set relatively extensively and irregularly. Consequently, a service maintenance person can implement maintenance subsequently only when paying certain learning costs. Based on this, there is a certain resource loss risk. In this process, attribute information of a service provider is a very important parameter, and can be used, after an order is generated, for processing such as determining whether the order is correct. However, different channels are used for different service lines, and service modes in different channels may also be different. Based on this, the attribute information of the service provider may be distributed randomly. Therefore, because a user refuses to pay, an unnecessary trouble is led to the user. Therefore, an effective solution is urgently needed, to resolve the above-mentioned problem.

SUMMARY

[0003] In view of this, embodiments of this specification provide a service processing method. One or more embodiments of this specification further relate to a service processing apparatus, a service processing system, a computing device, a computer-readable storage medium, and a computer program, to resolve a technical disadvantage in the conventional technology.

[0004] According to a first aspect of the embodiments of this specification, a service processing method is provided and applied to a service platform, including:

determining a service provider that participates in a target service;

reading service information and attribute information of the service provider, and building a channel contract associated with the target service based on the service information and the attribute information;

5 detecting a service participation credential of the service provider based on the channel contract; and

updating the service participation credential based on a detection result, and sending an updated service participation credential to a service participant of the target service.

10 **[0005]** In an optional embodiment, service identification information corresponding to the service provider is read, and the service identification information is used as attribute information of the service provider; and service range information and service mode information that correspond to the service provider are read and used as the service information of the service provider. The service identification information is used to locate the service provider, the service range information is used to determine a service range of the service provider, and the service mode information is used to verify a service mode.

15 **[0006]** In an optional embodiment, an initial channel contract associated with the target service is loaded; and the initial channel contract is updated based on the service identification information, the service range information, and the service mode information, to obtain the channel contract.

20 **[0007]** In an optional embodiment, a preset credential detection policy is extracted from the channel contract; the service participation credential of the service provider is loaded based on the attribute information; and the service participation credential is detected based on the credential detection policy.

25 **[0008]** In an optional embodiment, if the detection result is that detection succeeds, detection success information is added to the service participation credential, and the service participation credential to which the detection success information is added is used as the updated service participation credential; or if the detection result is that detection fails, credential error information is determined, an update policy corresponding to the credential error information is loaded, and the service participation credential is updated based on the update policy.

30 **[0009]** In an optional embodiment, the service user, the service provider, and the service object are determined based on the service participation order; object resource information associated with the service object is loaded, and credential registration information is determined based on the service user, the service provider, and the service object; and the service participation credential is created based on the credential registration information and the object resource information.

[0010] In an optional embodiment, the channel contract is parsed if the service provider is associated with resource space or an indirect resource management platform; and credential structure

verification logic corresponding to the service provider is determined based on a parsing result, and the credential detection policy is determined based on the credential structure verification logic.

[0011] In an optional embodiment, the channel contract is parsed when the service provider is associated with a direct resource management platform; and credential procedure verification logic
5 corresponding to the service provider is determined based on a parsing result, and the credential detection policy is determined based on the credential procedure verification logic.

[0012] According to a second aspect of the embodiments of this specification, a service processing apparatus is provided and applied to a service platform, including:

a determining module, configured to determine a service provider that participates in a
10 target service;

a reading module, configured to: read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information;

a detection module, configured to detect a service participation credential of the service
15 provider based on the channel contract; and

an update module, configured to: update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service.

[0013] According to a third aspect of the embodiments of this specification, a service processing
20 system is provided, and includes a service platform and a resource exchange platform, including:

the service platform is configured to: determine a service provider that participates in a target service; read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information; detect a service participation credential of the service provider based on the channel
25 contract; and update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service; and

the resource exchange platform is configured to: generate a resource exchange order based on the service participation credential, and send the resource exchange order to a service user who participates in the target service.

[0014] According to a fourth aspect of the embodiments of this specification, a computing device
30 is provided, including:

a memory and a processor, where

the memory is configured to store computer-executable instructions, and when the processor is configured to execute the computer-executable instructions, steps of the service processing method are implemented.

[0015] According to a fifth aspect of the embodiments of this specification, a computer-readable storage medium is provided. The computer-readable storage medium stores computer-executable instructions, and when the instructions are executed by a processor, steps of the service processing method are implemented.

[0016] According to a sixth aspect of the embodiments of this specification, a computer program is provided. When the computer program is executed on a computer, the computer is enabled to perform steps of the service processing method.

[0017] According to the service processing method provided in the embodiments, to reduce operation and maintenance costs of the service platform, verification logic can be unified, so that an order resource transfer of a downstream service is smoothly facilitated. After the service provider that participates in the target service is determined, the service information and the attribute information of the service provider can be read, the channel contract associated with the target service is built based on the service information and the attribute information, the service participation credential of the service provider is detected based on the channel contract, the service participation credential is updated based on the detection result, and the updated service participation credential is sent to the service participation party of the target service. In this way, the service participation credential is verified before being delivered by the service platform, to implement uniform verification on the credential, and reduce operation and maintenance costs of each participant of the target service. Based on this, verification is completed, to improve a success rate of the order resource transfer of the downstream service, and provide the user with a more convenient service.

BRIEF DESCRIPTION OF DRAWINGS

[0018] FIG. 1 is a schematic diagram illustrating a service processing method, according to an embodiment of this specification;

[0019] FIG. 2 is a flowchart illustrating a service processing method, according to an embodiment of this specification;

[0020] FIG. 3 is a schematic structural diagram illustrating a service processing apparatus, according to an embodiment of this specification;

[0021] FIG. 4 is a schematic structural diagram illustrating a service processing system, according to an embodiment of this specification;

[0022] FIG. 5 is a flowchart illustrating a processing process of a service processing method,

according to an embodiment of this specification; and

[0023] FIG. 6 is a structural block diagram illustrating a computing device, according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0024] Many specific details are set forth in the following description to facilitate full understanding of this specification. However, this specification can be implemented in many manners different from those described herein, and a person skilled in the art can make similar promotion without departing from the content of this specification, so that this specification is not limited to the specific implementations disclosed below.

[0025] Terms used in one or more embodiments of this specification are merely used to describe specific embodiments, and are not intended to limit the one or more embodiments of this specification. The terms "a" and "the" of singular forms used in one or more embodiments of this specification and the appended claims are also intended to include plural forms, unless otherwise specified in the context clearly. It should be further understood that the term "and/or" used in one or more embodiments of this specification refers to and includes any or all possible combinations of one or more associated listed items.

[0026] It should be understood that although terms "first", "second", etc. may be used in one or more embodiments of this specification to describe various types of information, the information is not limited to these terms. These terms are used merely to differentiate information of the same type. For example, the first may also be referred to as the second without departing from the scope of one or more embodiments of this specification, and similarly, the second may be referred to as the first. Depending on the context, the word "if" used herein may be interpreted as "when" or "while" or "in response to determining".

[0027] First, terms used in one or more embodiments of this specification are explained.

[0028] A merchant descriptor describes a merchant name.

[0029] "DBA" is short for "doing business as", and is used by card networks to mark a "brand" of a merchant or a part of a business license name. An obtaining manner of an acquiring institution is usually obtaining an on-boarding document of the merchant. Usually, the merchant sets a name of the DBA as a brand of the merchant.

[0030] This specification provides a service processing method. This specification further relates to a service processing apparatus, a service processing system, a computing device, a computer-readable storage medium, and a computer program. The service processing method, the service processing apparatus, the service processing system, the computing device, the computer-readable

storage medium, and the computer program are described in detail one by one in the following embodiments.

[0031] In actual applications, development of an international acquiring service has brought a more convenient service to a user. A merchant has more sources. Online acquiring, external acquiring, wallet acquiring, etc. are all sources for introducing the merchant. A tool of the merchant is also more intelligent and can be operated on a portal. Consequently, some technical problems are caused. Because different channels are used for different service lines, different service modes in different channel scenarios are different, and different service modes require different merchant names, the merchant name may be randomly assigned to the user. Consequently, when an order is transferred to the user, the user finds inconsistency through a check, and rejects payment. For example, the user purchases a game time card on a platform A, but a name B may be displayed in a bill, and an amount is 19.99 USD. After viewing the bill, the user finds that an order display name does not correspond to that on the platform, thereby rejecting payment. Therefore, an effective solution is urgently needed to resolve the above-mentioned problem.

[0032] Referring to a schematic diagram shown in FIG. 1, according to the service processing method provided in the embodiments, to reduce operation and maintenance costs of a service platform, verification logic can be unified, so that an order resource transfer of a downstream service is smoothly facilitated. After a service provider that participates in a target service is determined, service information and attribute information of the service provider can be read, a channel contract associated with the target service is built based on the service information and the attribute information, a service participation credential of the service provider is detected based on a channel contract, the service participation credential is updated based on the detection result, and an updated service participation credential is sent to the service participation party of the target service. In this way, the service participation credential is verified before being delivered by the service platform, to implement uniform verification on the credential, and reduce operation and maintenance costs of each participant of the target service. Based on this, verification is completed, to improve a success rate of the order resource transfer of the downstream service, and provide a user with a more convenient service.

[0033] FIG. 2 is a flowchart illustrating a service processing method, according to an embodiment of this specification. The method is applied to a service platform, and specifically includes the following steps.

[0034] Step S202: Determine a service provider that participates in a target service.

[0035] Specifically, the service platform is specifically a service platform that provides the target service, and includes but is not limited to a commodity procurement platform, a short video browsing

platform, a text information browsing platform, etc. It should be noted that the service platform needs to provide at least a resource transfer service. To be specific, a resource held by a user can be transferred, in an article transaction manner, to a service provider that provides an article. Correspondingly, the service provider is specifically a party, for example, a merchant, that provides a resource such as a commercially available commodity, a text, or a short video to a service user. The corresponding target service is specifically a service in which the user participates before the user and the service provider perform a resource transfer. The service can provide a commodity procurement service, a short video browsing service, a text information browsing service, etc. for the user. This is not limited in this embodiment here.

10 **[0036]** It should be noted that the service processing method provided in this embodiment is applied to an international acquiring service, and a name of the service provider is verified in a complex acquiring background, to satisfy use of a downstream service.

[0037] Based on this, after the service user submits an order, because of service complexity of the order, a plurality of parties need to jointly complete a resource transfer. In such a process, the service provider of the target service can be first determined on the service platform, to facilitate a subsequent verification processing operation, so as to reduce operation and maintenance costs of each participant of a service, and verify a related attribute of the service provider,

15 **[0038]** Further, in consideration that the service platform has a relatively strong concurrency capability, to avoid disorder in verifying each service provider, an implementation can be performed with reference to a service participation order associated with the service user. A specific implementation in this embodiment is as follows:

[0039] A service participation order is determined in response to a service participation request submitted by the service user for the target service; and a service object is determined in the service participation order, and a service provider of the service object is determined.

20 **[0040]** Specifically, the service user is specifically a user who participates in the target service. For example, in a commodity procurement scenario, the service user is a user who purchases a commodity on the commodity procurement platform. Alternatively, in a short video scenario, the service user is a user who watches a video by using short video playback software. Correspondingly, the target service is specifically a service that can be provided to the service user, and includes but is not limited to a commodity procurement service, a short video playback service, a text information browsing service, etc. Correspondingly, the service participation request is specifically a request submitted when the service user participates in the target service. A subsequent service operation can be triggered based on the request. For example, in the commodity procurement scenario, the service participation request can be a purchase request submitted when the user purchases the commodity.

30

Alternatively, in the video playback scenario, the service participation request can be a playback request submitted when the user plays back the video.

5 [0041] Correspondingly, the service participation order is specifically an order generated for a service participation request currently submitted by the service user, and the order is used to record information related to a target service in which the service user currently participates, and includes but is not limited to an identity of the service user, resource consumption information, object information, etc. Correspondingly, the service object is specifically an object hit when the service user participates in the target service. For example, in the commodity procurement scenario, the service object can be a commodity selected and purchased by the user. For example, in the short video
10 playback scenario, the service object can be a video played by the user.

[0042] Based on this, to accurately determine the service provider, the service participation order can be determined in response to the service participation request submitted by the service user for the target service; and the service object is determined in the service participation order, and the service provider of the service object is determined, to facilitate subsequent use.

15 [0043] In conclusion, the service provider is determined with reference to the service participation order, to improve accuracy of determining the service provider, thereby facilitating subsequent use.

[0044] Step S204: Read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information.

20 [0045] Specifically, after the service provider is determined, to accurately detect a service participation credential of the service provider, the service information and the attribute information of the service provider can be read, and the channel contract associated with the target service is built based on the service information and the attribute information, to facilitate verification based on the channel contract.

25 [0046] The service information is specifically information describing a service provided by the service provider, and can be used to locate the service provider, and determine a service type and range that are provided by the service provider, etc. Correspondingly, the attribute information is specifically basic attribute information of the service provider, and is used to ensure, when the channel contract is built, that the channel contract is associated with the service provider, so that verification
30 can be subsequently performed based on the channel contract.

[0047] Further, when the service information and the attribute information are determined, to locate a specific service provider and further improve mode verification accuracy, the service information and the attribute information can be determined with reference to service identification information, service range information, and service mode information. In this embodiment, a specific

implementation is as follows:

[0048] Service identification information corresponding to the service provider is read and used as attribute information of the service provider; and service range information and service mode information that correspond to the service provider are read and used as the service information of the service provider. The service identification information is used to locate the service provider, the service range information is used to determine a service range of the service provider, and the service mode information is used to verify a service mode.

[0049] Specifically, the service identification information is specifically information corresponding to an identity of the service provider, and is unique. Correspondingly, the service range information is specifically information describing the service range provided by the service provider, and can be used to perform properness verification on the service range. Correspondingly, the service mode information is specifically information describing a service mode of the service provider, and can be used to verify the service mode.

[0050] Based on this, the service identification information corresponding to the service provider can be read and used as the attribute information of the service provider; and the service range information and the service mode information that correspond to the service provider are read and used as the service information of the service provider. The service identification information can be used to locate the service provider, the service range information can be used to determine a service range of the service provider, and the service mode information can be used to verify the service mode.

[0051] For example, in an international service scenario, the service identification information is a merchant ID or a merchant identifier, and a specific merchant can be located. The service range information is service range information of the merchant, and can be embodied as an internal service of a group or an external service of a group. The service mode information is a merchant service mode, and correctness of the mode can be further verified, to subsequently verify a merchant name with reference to the service identification information, the service range information, and the service mode information, thereby ensuring, when the user pays for an order, that a to-be-paid merchant is a merchant corresponding to a shopping requirement of the user.

[0052] In conclusion, the service information and the attribute information are determined with reference to the service identification information, the service mode information, and the service range information, to facilitate subsequent use, so that a channel contract that matches a current service scenario is built for use.

[0053] Further, when the channel contract is built, the channel contract can be built based on the above-mentioned information, to complete verification of the service participation credential from a

plurality of dimensions. In this embodiment, a specific implementation is as follows:

[0054] An initial channel contract associated with the target service is loaded; and the initial channel contract is updated based on the service identification information, the service range information, and the service mode information, to obtain the channel contract.

5 **[0055]** Specifically, the initial channel contract is specifically a channel contract that is set for the target service, and the channel contract can be directly used to verify the service participation credential. However, accuracy of later verification is higher when verification is performed with reference to the service identification information, the service range information, and the service mode information.

10 **[0056]** Based on this, the initial channel contract associated with the target service can be loaded; and then, the initial channel contract is updated based on the service identification information, the service range information, and the service mode information, to obtain the channel contract.

[0057] For example, in the international service scenario, a channel contract in a financial exchange field of the payment platform has had a logical condition for determining a correct and proper merchant bill name. Based on this, to ensure that precision of verification is further improved, the read service identification information, the read service range information, and the read service mode information can be updated to an existing channel contract, to obtain, for subsequent use, a channel contract corresponding to a current scenario.

15 **[0058]** In actual applications, when the service identification information, the service range information, and the service mode information are fused into a preset initial channel contract, parameter assignment processing can be performed based on preset execution logic, so that after the service identification information, the service range information, and the service mode information are written into the channel contract, the channel contract can run and be used subsequently. The preset execution logic can be set based on an actual requirement. This is not limited in this embodiment.

20 **[0059]** In conclusion, in an international service in actual applications, the initial channel contract of the service platform has had the logical condition for determining the correct and proper merchant bill name. Therefore, corresponding attribute information, etc. is added based on this, to build a channel contract corresponding to a current service scenario for use.

30 **[0060]** Step S206: Detect a service participation credential of the service provider based on the channel contract.

[0061] Specifically, after the channel contract is built, to detect the service participation credential before the user performs a resource transfer, and prevent the order from being unable to be completed, the service participation credential can be preliminarily detected based on the channel contract, so

that the user can be replaced to perform preliminary detection before the resource transfer.

[0062] The service participation credential is specifically a resource transfer credential that includes the name of the service provider. The service user can verify, based on the service participation credential, whether a receiver of the resource transfer is the service provider, to check an identity during the resource transfer. Based on this, after the channel contract is obtained, to avoid a problem that the service user refuses to perform the resource transfer, the service participant credential of the service provider can be detected based on the channel contract, to facilitate subsequent use.

[0063] In a specific implementation, different service scenarios are related to different services, service ranges, and service modes. Therefore, when the service participation credential is detected based on the channel contract, the service participation credential can be detected based on an actual requirement by selecting different detection dimensions, to ensure that the service participation credential can be fully detected in a current service scenario, thereby reducing a detection operation performed by the user before the user performs the resource transfer, and improving a resource transfer success rate.

[0064] To implement accurate detection of the service participation credential, the service participation credential can be detected after being determined. In this embodiment, a specific implementation is as follows:

[0065] The service user, the service provider, and the service object are determined based on the service participation order; object resource information associated with the service object is loaded, and credential registration information is determined based on the service user, the service provider, and the service object; and the service participation credential is created based on the credential registration information and the object resource information.

[0066] Specifically, the object resource information is specifically a resource that needs to be consumed when the service object is transferred, and the object resource information can be description information consumed by a computer resource, capital consumption information corresponding to a commodity transaction, corresponding bandwidth consumption information existing when a short video is played back, etc. Correspondingly, the credential registration information is specifically related information used to record an order credential existing when a resource transfer is performed between the service user, the service provider, and the service object.

[0067] Based on this, the service user, service provider, and service object can be determined according to the service participation order for accurate detection. Then, the object resource information associated with the service object is loaded, and the credential registration information is determined according to the service user, the service provider, and the service object. Finally, a

service participation credential is created based on the credential registration information and the object resource information, so as to facilitate detection by using a channel contract.

[0068] For example, the user purchases a game time card of a game of a country M on a platform A in a country C. A current of the country M needs to be used to complete such a payment process. A currency of the country C and the currency of the country M are different. The amount is 19.99. Based on this, after the user purchases the game point card, it is determined that an amount of 19.99 needs to be transferred to a merchant that provides the game point card, and the amount corresponds to the currency of the country M. Then, when an order is secure, to ensure that the user can complete the order when performing payment, payment credential information of the game time card can be created based on a purchased commodity {game time card}, information about the platform A, and user information, to create a purchase credential corresponding to the game time card with reference to a payment amount and the payment credential information, help subsequently detect the purchase credential based on the channel contract, and reduce a verification operation performed by the user when the user performs payment.

[0069] In conclusion, the service participation credential is built with reference to the credential registration information and the object resource information, so that information that needs to be checked by the service user can be put into the credential, thereby helping the service user to perform identity authentication.

[0070] Further, when the service participation credential is verified, in consideration that different service providers may correspond to different service participation credentials, and different service participation credentials need to be detected with reference to different credential detection policies, a credential detection policy corresponding to a current scenario needs to be selected to implement detection. In this embodiment, a specific implementation is as follows:

[0071] A preset credential detection policy is extracted from the channel contract; the service participation credential of the service provider is loaded based on the attribute information; and the service participation credential is detected based on the credential detection policy.

[0072] Specifically, the credential detection policy is specifically a policy used to detect different types of service participation credentials. In a specific implementation, different credential detection policies can be set based on an actual requirement, to detect any type of service participation credential. This is not limited in this embodiment.

[0073] Based on this, during detection, targeted selection can be performed. To be specific, the preset credential detection policy can be extracted from the channel contract; the service participation credential of the service provider is loaded based on the attribute information; and the service participation credential is detected based on the credential detection policy.

[0074] Further, different credential detection policies can be implemented in the following manner:

[0075] (1) The channel contract is parsed if the service provider is associated with resource space or an indirect resource management platform; and credential structure verification logic corresponding to the service provider is determined based on a parsing result, and the credential detection policy is determined based on the credential structure verification logic.

[0076] Based on this, when the service provider is associated with the resource space or the indirect resource management platform, it indicates that the service provider may be a wallet or a secondary agent. Therefore, the channel contract can be parsed. The credential structure verification logic corresponding to the service provider is determined based on the parsing result, and the credential detection policy is determined based on the credential structure verification logic. A name structure of the service provider in the service participation credential is detected based on the credential structure verification logic.

[0077] For example, if the service provider is SDWO, XXXXX (SDWO NAME) * XXXX (MERCHANT NAME) is selected as verification logic corresponding to the service provider, it is determined that the service provider corresponds to APAYHK * AEXPRESS, and APAYHK * AEXPRESS corresponding to the service provider is detected based on the verification logic. If detection succeeds, it indicates that a merchant name in a subsequent payment order is consistent with that of a merchant that provides a commodity, to help the user to perform payment.

[0078] For another example, if the service provider is PF, XXXXX (PFNAME) * XXXX (MERCHANT NAME) can be selected as verification logic corresponding to the service provider, and it is determined that the service provider corresponds to YM * AEXPRESS, where it represents that YM is PF and AEXPRESS is a merchant. In this case, YM * AEXPRESS corresponding to the service provider can be detected based on the verification logic. If detection succeeds, it indicates that a merchant name in a subsequent payment order is consistent with that of a merchant that provides a commodity, to help the user to perform payment.

[0079] (2) The channel contract is parsed when the service provider is associated with a direct resource management platform; and credential procedure verification logic corresponding to the service provider is determined based on a parsing result, and the credential detection policy is determined based on the credential procedure verification logic.

[0080] Based on this, if the service provider is associated with the direct resource management platform, it indicates that the service provider may be a specific merchant, a specific payment platform, or a specific acquiring institution. Therefore, the channel contract can be parsed; and the credential procedure verification logic corresponding to the service provider is determined based on

the parsing result, and the credential detection policy is determined based on the credential procedure verification logic. A name structure of the service provider in the service participation credential is detected based on the credential procedure verification logic.

[0081] For example, if the service provider is AMEX, verification logic corresponding to the service provider is selected as follows: 1. A merchant, an acquiring institution, and a plurality of MIDs specified for different regions need to be preset in a file of an acquiring GFSG of AMEX. Each region in a case of each identity is displayed in a bill of the user. 2. A transaction is sent to a financial institution. Verification is performed based on an acquiring region and a PID of the merchant, to configure an MID applicable to a merchant region, and the MID is uploaded to AMEX. A rule is XXXXXX (MERCHANT NAME) SINGAPORE, and it is determined that the service provider corresponds to A SINGAPORE and A EU. In this case, A SINGAPORE and A EU corresponding to the service provider can be detected based on the above-mentioned rule. If detection succeeds, it indicates that a merchant name in a subsequent payment order is consistent with that of a merchant that provides a commodity, to help the user to perform payment.

[0082] In conclusion, verification is performed in different manners, the transaction can be checked before being delivered to the acquiring institution, and a corresponding replacement is made, to reduce operation and maintenance costs, thereby increasing flexibility of the international acquiring service.

[0083] Step S208: Update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service.

[0084] Specifically, after the service participation credential is detected based on the channel contract, the service participation credential can be updated based on the detection result, to obtain a service participation credential that satisfies a use requirement, and the updated service participation credential is sent to the service participant of the target service.

[0085] Further, when the service participation credential is updated, update can be completed with reference to detection success information, to feed back a correct service participation credential to the service participant, thereby reducing a problem that the service user rejects the resource transfer. In this embodiment, a specific implementation is as follows:

[0086] If the detection result is that detection succeeds, the detection success information is added to the service participation credential, and the service participation credential to which the detection success information is added is used as the updated service participation credential.

[0087] If the detection result is that detection fails, credential error information is determined, an update policy corresponding to the credential error information is loaded, and the service participation credential is updated based on the update policy.

[0088] Based on this, if the detection result is that detection succeeds, it indicates that no problem exists. In this case, the detection success information can be added to the service participation credential, and the service participation credential to which the detection success information is added is used as the updated service participation credential; and the updated service participation credential is sent to the service participant. If the detection result is that detection fails, it indicates that a problem exists. In this case, the credential error information can be determined, the update policy corresponding to the credential error information is loaded, and the service participation credential is updated based on the update policy, to send, to the service participation party, a result obtained after update.

10 [0089] In conclusion, the service participation credential is updated, to reduce subsequent operation and maintenance costs on an institution side, increase flexibility of the international service, unify processing logic, help improve an overall transaction processing success rate, and reduce an unnecessary and redundant MID.

[0090] According to the service processing method provided in this embodiment, to reduce operation and maintenance costs of the service platform, verification logic can be unified, so that an order resource transfer of a downstream service is smoothly facilitated. After the service provider that participates in the target service is determined, the service information and the attribute information of the service provider can be read, the channel contract associated with the target service is built based on the service information and the attribute information, the service participation credential of the service provider is detected based on the channel contract, the service participation credential is updated based on the detection result, and the updated service participation credential is sent to the service participation party of the target service. In this way, the service participation credential is verified before being delivered by the service platform, to implement uniform verification on the credential, and reduce operation and maintenance costs of each participant of the target service. Based on this, verification is completed, to improve a success rate of the order resource transfer of the downstream service, and provide the user with a more convenient service.

20 [0091] Corresponding to the method embodiment, this specification further provides an embodiment of a service processing apparatus. FIG. 3 is a schematic structural diagram illustrating a service processing apparatus, according to an embodiment of this specification. As shown in FIG. 3, the apparatus is applied to a service platform, and includes:

a determining module 302, configured to determine a service provider that participates in a target service;

a reading module 304, configured to: read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information;

5 a detection module 306, configured to detect a service participation credential of the service provider based on the channel contract; and

an update module 308, configured to: update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service.

[0092] In an optional embodiment, the determining module 302 is further configured to:

10 determine a service participation order in response to a service participation request submitted by a service user for the target service; and determine a service object in the service participation order, and determining a service provider of the service object.

[0093] In an optional embodiment, the reading module 304 is further configured to:

15 read service identification information corresponding to the service provider, and use the service identification information as attribute information of the service provider; and read service range information and service mode information that correspond to the service provider, and use the service range information and the service mode information as the service information of the service provider, where the service identification information is used to locate the service provider, the service range information is used to determine a service range of the service provider, and the service
20 mode information is used to verify a service mode.

[0094] In an optional embodiment, the reading module 304 is further configured to:

load an initial channel contract associated with the target service; and update the initial channel contract based on the service identification information, the service range information, and the service mode information, to obtain the channel contract.

25 **[0095]** In an optional embodiment, the detection module 306 is further configured to:

extract a preset credential detection policy from the channel contract; load the service participation credential of the service provider based on the attribute information; and detect the service participation credential based on the credential detection policy.

[0096] In an optional embodiment, the update module 308 is further configured to:

30 if the detection result is that detection succeeds, add detection success information to the service participation credential, and use, as the updated service participation credential, the service participation credential to which the detection success information is added; or if the detection result is that detection fails, determining credential error information, load an update policy corresponding

to the credential error information, and update the service participation credential based on the update policy.

[0097] In an optional embodiment, determining the service participation credential includes:

determine the service user, the service provider, and the service object based on the service participation order; load object resource information associated with the service object, and determine credential registration information based on the service user, the service provider, and the service object; and create the service participation credential based on the credential registration information and the object resource information.

[0098] In an optional embodiment, the detection module 306 is further configured to:

parse the channel contract if the service provider is associated with resource space or an indirect resource management platform; and determine, based on a parsing result, credential structure verification logic corresponding to the service provider, and determine the credential detection policy based on the credential structure verification logic.

[0099] In an optional embodiment, the detection module 306 is further configured to:

parse the channel contract when the service provider is associated with a direct resource management platform; and determine, based on a parsing result, credential procedure verification logic corresponding to the service provider, and determine the credential detection policy based on the credential procedure verification logic.

[0100] In conclusion, to reduce operation and maintenance costs of the service platform, verification logic can be unified, so that an order resource transfer of a downstream service is smoothly facilitated. After the service provider that participates in the target service is determined, the service information and the attribute information of the service provider can be read, the channel contract associated with the target service is built based on the service information and the attribute information, the service participation credential of the service provider is detected based on the channel contract, the service participation credential is updated based on the detection result, and the updated service participation credential is sent to the service participation party of the target service. In this way, the service participation credential is verified before being delivered by the service platform, to implement uniform verification on the credential, and reduce operation and maintenance costs of each participant of the target service. Based on this, verification is completed, to improve a success rate of the order resource transfer of the downstream service, and provide the user with a more convenient service.

[0101] A schematic solution of the service processing apparatus in the embodiments is described above. It should be noted that the technical solution of the service processing apparatus and the technical solution of the service processing method belong to the same concept. For detailed content

not described in detail in the technical solution of the service processing apparatus, references can be made to descriptions of the technical solution of the service processing method.

[0102] Corresponding to the method embodiment, this specification further provides an embodiment of a service processing system. FIG. 4 is a schematic structural diagram illustrating a service processing system, according to an embodiment of this specification. As shown in FIG. 4, a service processing system 400 includes a service platform 410 and a resource exchange platform 420, including:

[0103] The service platform 410 is configured to: determine a service provider that participates in a target service; read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information; detect a service participation credential of the service provider based on the channel contract; and update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service.

[0104] The resource exchange platform 420 is configured to: generate a resource exchange order based on the service participation credential, and send the resource exchange order to a service user who participates in the target service.

[0105] In an optional embodiment, the service platform 410 is configured to: determine a service participation order in response to a service participation request submitted by the service user for the target service; and determine a service object in the service participation order, and determine a service provider of the service object.

[0106] In an optional embodiment, the service platform 410 is configured to: read service identification information corresponding to the service provider, and use the service identification information as attribute information of the service provider; and read service range information and service mode information that correspond to the service provider, and use the service range information and the service mode information as the service information of the service provider. The service identification information is used to locate the service provider, the service range information is used to determine a service range of the service provider, and the service mode information is used to verify a service mode.

[0107] In an optional embodiment, the service platform 410 is configured to: load an initial channel contract associated with the target service; and update the initial channel contract based on the service identification information, the service range information, and the service mode information, to obtain the channel contract.

[0108] In an optional embodiment, the service platform 410 is configured to: extract a preset credential detection policy from the channel contract; load the service participation credential of the

service provider based on the attribute information; and detect the service participation credential based on the credential detection policy.

[0109] In an optional embodiment, the service platform 410 is configured to: if the detection result is that detection succeeds, add detection success information to the service participation credential, and use, as the updated service participation credential, the service participation credential to which the detection success information is added; or if the detection result is that detection fails, determining credential error information, load an update policy corresponding to the credential error information, and update the service participation credential based on the update policy.

[0110] In an optional embodiment, the service platform 410 is configured to: determine the service user, the service provider, and the service object based on the service participation order; load object resource information associated with the service object, and determine credential registration information based on the service user, the service provider, and the service object; and create the service participation credential based on the credential registration information and the object resource information.

[0111] In an optional embodiment, the service platform 410 is configured to: parse the channel contract if the service provider is associated with resource space or an indirect resource management platform; and determine, based on a parsing result, credential structure verification logic corresponding to the service provider, and determine the credential detection policy based on the credential structure verification logic.

[0112] In an optional embodiment, the service platform 410 is configured to: parse the channel contract when the service provider is associated with a direct resource management platform; and determine, based on a parsing result, credential procedure verification logic corresponding to the service provider, and determine the credential detection policy based on the credential procedure verification logic.

[0113] In conclusion, to reduce operation and maintenance costs of the service platform, verification logic can be unified, so that an order resource transfer of a downstream service is smoothly facilitated. After the service provider that participates in the target service is determined, the service information and the attribute information of the service provider can be read, the channel contract associated with the target service is built based on the service information and the attribute information, the service participation credential of the service provider is detected based on the channel contract, the service participation credential is updated based on the detection result, and the updated service participation credential is sent to the service participation party of the target service. In this way, the service participation credential is verified before being delivered by the service platform, to implement uniform verification on the credential, and reduce operation and maintenance

costs of each participant of the target service. Based on this, verification is completed, to improve a success rate of the order resource transfer of the downstream service, and provide the user with a more convenient service.

[0114] A schematic solution of the service processing system in the embodiments is described above. It should be noted that the technical solution of the service processing system and the technical solution of the service processing method belong to the same concept. For detailed content not described in detail in the technical solution of the service processing system, references can be made to descriptions of the technical solution of the service processing method.

[0115] With reference to FIG. 5, the following further describes the service processing method by using an example that the service processing method provided in this specification is applied to a merchant name verification scenario. FIG. 5 is a flowchart illustrating a processing process of a service processing method, according to an embodiment of this specification. The method specifically includes the following steps.

[0116] Step S502: Determine a service participation order in response to a service participation request submitted by a service user for a target service.

[0117] Step S504: Determine a service object in the service participation order, and determine a service provider of the service object.

[0118] Step S506: Read service identification information corresponding to the service provider, and use the service identification information as attribute information of the service provider.

[0119] Step S508: Read service range information and service mode information that correspond to the service provider, and use the service range information and the service mode information as service information of the service provider.

[0120] Step S510: Load an initial channel contract associated with the target service.

[0121] Step S512: Update the initial channel contract based on the attribute information, the service range information, and the service mode information, to obtain a channel contract.

[0122] Step S514: Extract a preset credential detection policy from the channel contract.

[0123] Step S516: Load a service participation credential of the service provider based on the attribute information.

[0124] Step S518: Detect the service participation credential based on the credential detection policy.

[0125] Step S520: Update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service.

[0126] For example, if the service provider is SDWO, XXXXX (SDWO NAME) * XXXX (MERCHANT NAME) is selected as verification logic corresponding to the service provider, it is

determined that the service provider corresponds to APAYHK * AEXPRESS, and APAYHK * AEXPRESS corresponding to the service provider is detected based on the verification logic. If detection succeeds, it indicates that a merchant name in a subsequent payment order is consistent with that of a merchant that provides a commodity, to help the user to perform payment.

5 [0127] Alternatively, if the service provider is PF, XXXXX (PFNAME) * XXXX (MERCHANT NAME) can be selected as verification logic corresponding to the service provider, and it is determined that the service provider corresponds to YM * AEXPRESS, where it represents that YM is PF and AEXPRESS is a merchant. In this case, YM * AEXPRESS corresponding to the service provider can be detected based on the verification logic. If detection succeeds, it indicates that a
10 merchant name in a subsequent payment order is consistent with that of a merchant that provides a commodity, to help the user to perform payment.

[0128] Alternatively, if the service provider is AMEX, verification logic corresponding to the service provider is selected as follows: 1. A merchant, an acquiring institution, and a plurality of
15 MIDs specified for different regions need to be preset in a file of an acquiring GFSG of AMEX. Each region in a case of each identity is displayed in a bill of the user. 2. A transaction is sent to a financial institution. Verification is performed based on an acquiring region and a PID of the merchant, to configure an MID applicable to a merchant region, and the MID is uploaded to AMEX. A rule is
XXXXXX (MERCHANT NAME) SINGAPORE, and it is determined that the service provider corresponds to A SINGAPORE and A EU. In this case, A SINGAPORE and A EU corresponding to
20 the service provider can be detected based on the above-mentioned rule. If detection succeeds, it indicates that a merchant name in a subsequent payment order is consistent with that of a merchant that provides a commodity, to help the user to perform payment.

[0129] In conclusion, to reduce operation and maintenance costs of the service platform, verification logic can be unified, so that an order resource transfer of a downstream service is
25 smoothly facilitated. After the service provider that participates in the target service is determined, the service information and the attribute information of the service provider can be read, the channel contract associated with the target service is built based on the service information and the attribute information, the service participation credential of the service provider is detected based on the channel contract, the service participation credential is updated based on the detection result, and the
30 updated service participation credential is sent to the service participation party of the target service. In this way, the service participation credential is verified before being delivered by the service platform, to implement uniform verification on the credential, and reduce operation and maintenance costs of each participant of the target service. Based on this, verification is completed, to improve a success rate of the order resource transfer of the downstream service, and provide the user with a

more convenient service.

[0130] FIG. 6 is a structural block diagram illustrating a computing device 600, according to an embodiment of this specification. Components of the computing device 600 include but are not limited to a memory 610 and a processor 620. The processor 620 and the memory 610 are connected by using a bus 630, and a database 650 is configured to store data.

[0131] The computing device 600 further includes an access device 640. The access device 640 enables the computing device 600 to communicate via one or more networks 660. Examples of these networks include a public switched telephone network (PSTN), a local area network (LAN), a wide area network (WAN), a personal access network (PAN), or a combination of communication networks such as the Internet. The access device 640 can include one or more of any types of wired or wireless network interfaces (for example, a network interface controller (NIC)) such as an IEEE 802.11 wireless local area network (WLAN) wireless interface, a worldwide interoperability for microwave access (Wi-MAX) interface, an Ethernet interface, a universal serial bus (USB) interface, a cellular network interface, a Bluetooth interface, and a near field communication (NFC) interface.

[0132] In an embodiment of the present application, the components of the computing device 600 and other components not shown in FIG. 6 can also be connected to each other, for example, through a bus. It should be understood that the structural block diagram of the computing device shown in FIG. 6 is for an illustrative purpose only and is not intended to limit the scope of this application. A person skilled in the art can add or replace other components as needed. The computing device 600 can be any type of stationary or mobile computing device, including a mobile computer or a mobile computing device (for example, a tablet computer, a personal digital assistant, a laptop computer, a notebook computer, or a netbook), a mobile phone (for example, a smartphone), a wearable computing device (for example, a smart watch or smart glasses), or other types of mobile devices, or a stationary computing device such as a desktop computer or a personal computer (PC). The computing device 600 can alternatively be a mobile or stationary server.

[0133] The processor 620 is configured to execute computer-executable instructions, and when the computer-executable instructions are executed by the processor, the following method is implemented:

determining a service provider that participates in a target service;

reading service information and attribute information of the service provider, and building a channel contract associated with the target service based on the service information and the attribute information;

detecting a service participation credential of the service provider based on the channel contract; and

updating the service participation credential based on a detection result, and sending an updated service participation credential to a service participant of the target service.

[0134] In an optional embodiment, service identification information corresponding to the service provider is read and used as attribute information of the service provider; and service range information and service mode information that correspond to the service provider are read and used as the service information of the service provider. The service identification information is used to locate the service provider, the service range information is used to determine a service range of the service provider, and the service mode information is used to verify a service mode.

[0135] In an optional embodiment, an initial channel contract associated with the target service is loaded; and the initial channel contract is updated based on the service identification information, the service range information, and the service mode information, to obtain the channel contract. In an optional embodiment, a preset credential detection policy is extracted from the channel contract; the service participation credential of the service provider is loaded based on the attribute information; and the service participation credential is detected based on the credential detection policy.

[0136] In an optional embodiment, if the detection result is that detection succeeds, detection success information is added to the service participation credential, and the service participation credential to which the detection success information is added is used as the updated service participation credential; or if the detection result is that detection fails, determining credential error information, an update policy corresponding to the credential error information is loaded, and the service participation credential is updated based on the update policy.

[0137] In an optional embodiment, the service user, the service provider, and the service object are determined based on the service participation order; object resource information associated with the service object is loaded, and credential registration information is determined based on the service user, the service provider, and the service object; and the service participation credential is created based on the credential registration information and the object resource information.

[0138] In an optional embodiment, the channel contract is parsed if the service provider is associated with resource space or an indirect resource management platform; and credential structure verification logic corresponding to the service provider is determined based on a parsing result, and the credential detection policy is determined based on the credential structure verification logic.

[0139] In an optional embodiment, the channel contract is parsed when the service provider is associated with a direct resource management platform; and credential procedure verification logic corresponding to the service provider is determined based on a parsing result, and the credential detection policy is determined based on the credential procedure verification logic.

[0140] A schematic solution of the computing device of the embodiments is described above. It

should be noted that the technical solution of the computing device and the technical solution of the service processing method belong to the same concept. For detailed content not described in detail in the technical solution of the computing device, references can be made to the descriptions of the technical solution of the service processing method.

5 [0141] An embodiment of this specification further provides a computer-readable storage medium. The computer-readable storage medium stores computer-executable instructions, and when the computer-executable instructions are executed by a processor, steps of the service processing method are implemented.

10 [0142] A schematic solution of the computer-readable storage medium in the embodiments is described above. It should be noted that the technical solution of the storage medium and the technical solution of the service processing method belong to the same concept. For detailed content not described in detail in the technical solution of the storage medium, references can be made to descriptions of the technical solution of the service processing method.

15 [0143] An embodiment of this specification further provides a computer program. When the computer program is executed on a computer, the computer is enabled to perform steps of the service processing method.

20 [0144] A schematic solution of the computer program in the embodiments is described above. It should be noted that the technical solution of the computer program and the technical solution of the service processing method belong to the same concept. For detailed content not described in detail in the technical solution of the storage medium, references can be made to descriptions of the technical solution of the service processing method.

25 [0145] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, processes described in the accompanying drawings do not necessarily need a specific order or a sequential order shown to achieve the desired results. In some implementations, multi-tasking and concurrent processing are feasible or may be advantageous.

30 [0146] The computer instructions include computer program code, and the computer program code may be in a source code form, an object code form, an executable file form, some intermediate forms, etc. The computer-readable medium may include any entity or apparatus capable of carrying the computer program code, a recording medium, a USB flash drive, a removable hard disk, a magnetic disk, an optical disc, a computer memory, a read-only memory (ROM), a random access memory (RAM), an electrical carrier signal, a telecommunication signal, a software distribution medium, etc. It should be noted that the content contained in the computer-readable medium can be

appropriately increased or decreased in accordance with the requirements of the legislation and patent practice in the jurisdiction, for example, in some jurisdictions, the computer-readable medium does not include electrical carrier signals or telecommunication signals in accordance with the legislation and patent practice.

5 **[0147]** It should be noted that, for a brief description, the above-mentioned method embodiments are represented as a series of actions. However, a person skilled in the art should understand that some embodiments of this specification are not limited to the described order of the actions, because according to some embodiments of this specification, some steps can be performed in another order or simultaneously. In addition, a person skilled in the art should also understand that all the
10 embodiments described in this specification are example embodiments, and the related actions and modules are not necessarily mandatory to some embodiments of this specification.

[0148] In the above-mentioned embodiments, the descriptions of the embodiments have respective focuses. For a part that is not described in detail in an embodiment, references can be made to related descriptions in other embodiments.

15 **[0149]** The example embodiments of this specification disclosed above are intended merely to help describe this specification. The optional embodiments do not describe all the details in detail, nor do they limit the present invention to the specific implementations described. Clearly, many modifications and changes can be made based on the content of some embodiments of this specification. These embodiments are selected and described in detail in this specification in order to
20 better explain the principles and practical applications of some embodiments of this specification, so that a person skilled in the art can well understand and use this specification. This specification is limited only by the claims and their full scope and equivalents.

CLAIMS

What is claimed is:

1. A service processing method, applied to a service platform, comprising:
determining a service provider that participates in a target service;
5 reading service information and attribute information of the service provider, and building a channel contract associated with the target service based on the service information and the attribute information;
detecting a service participation credential of the service provider based on the channel contract;
and
10 updating the service participation credential based on a detection result, and sending an updated service participation credential to a service participant of the target service.
2. The method according to claim 1, wherein the determining a service provider that participates in a target service comprises:
determining a service participation order in response to a service participation request submitted
15 by a service user for the target service; and
determining a service object in the service participation order, and determining a service provider of the service object.
3. The method according to claim 1, wherein the reading service information and attribute information of the service provider comprises:
20 reading service identification information corresponding to the service provider, and using the service identification information as attribute information of the service provider; and
reading service range information and service mode information that correspond to the service provider, and using the service range information and the service mode information as the service information of the service provider, wherein
25 the service identification information is used to locate the service provider, the service range information is used to determine a service range of the service provider, and the service mode information is used to verify a service mode.
4. The method according to claim 3, wherein the building a channel contract associated with the target service based on the service information and the attribute information comprises:
30 loading an initial channel contract associated with the target service; and
updating the initial channel contract based on the service identification information, the service range information, and the service mode information, to obtain the channel contract.
5. The method according to any one of claims 1 to 4, wherein the detecting a service participation credential of the service provider based on the channel contract comprises:

extracting a preset credential detection policy from the channel contract;

loading the service participation credential of the service provider based on the attribute information; and

detecting the service participation credential based on the credential detection policy.

5 6. The method according to claim 1, wherein the updating the service participation credential based on a detection result comprises:

if the detection result is that detection succeeds, adding detection success information to the service participation credential, and using, as the updated service participation credential, the service participation credential to which the detection success information is added; or

10 if the detection result is that detection fails, determining credential error information, loading an update policy corresponding to the credential error information, and updating the service participation credential based on the update policy.

7. The method according to claim 2, wherein determining the service participation credential comprises:

15 determining the service user, the service provider, and the service object based on the service participation order;

loading object resource information associated with the service object, and determining credential registration information based on the service user, the service provider, and the service object; and

20 creating the service participation credential based on the credential registration information and the object resource information.

8. The method according to claim 5, wherein the extracting a preset credential detection policy from the channel contract comprises:

25 parsing the channel contract if the service provider is associated with resource space or an indirect resource management platform; and

determining, based on a parsing result, credential structure verification logic corresponding to the service provider, and determining the credential detection policy based on the credential structure verification logic.

30 9. The method according to claim 5, wherein the extracting a preset credential detection policy from the channel contract comprises:

parsing the channel contract when the service provider is associated with a direct resource management platform; and

determining, based on a parsing result, credential procedure verification logic corresponding to the service provider, and determining the credential detection policy based on the credential procedure

verification logic.

10. A service processing apparatus, applied to a service platform, comprising:

a determining module, configured to determine a service provider that participates in a target service;

5 a reading module, configured to: read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information;

a detection module, configured to detect a service participation credential of the service provider based on the channel contract; and

10 an update module, configured to: update the service participation credential based on a detection result, and send an updated service participation credential to a service participant of the target service.

11. A service processing system, comprising a service platform and a resource exchange platform, wherein:

15 the service platform is configured to: determine a service provider that participates in a target service; read service information and attribute information of the service provider, and build a channel contract associated with the target service based on the service information and the attribute information; detect a service participation credential of the service provider based on the channel contract; and update the service participation credential based on a detection result, and send an
20 updated service participation credential to a service participant of the target service; and

the resource exchange platform is configured to: generate a resource exchange order based on the service participation credential, and send the resource exchange order to a service user who participates in the target service.

12. A computing device, comprising:

25 a memory and a processor, wherein

the memory is configured to store computer-executable instructions, the processor is configured to execute the computer-executable instructions, and when the computer-executable instructions are executed by the processor, steps of the method according to any one of claims 1 to 9 are implemented.

30 13. A computer-readable storage medium, wherein the computer-readable storage medium stores computer-executable instructions, and when the computer-executable instructions are executed by a processor, steps of the method according to any one of claims 1 to 9 are implemented.