



**ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

**(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ**

(21)(22) Заявка: 2018137487, 20.03.2017

Приоритет(ы):

(30) Конвенционный приоритет:  
25.03.2016 CN 201610180030.4

(43) Дата публикации заявки: 27.04.2020 Бюл. № 12

(85) Дата начала рассмотрения заявки РСТ на  
национальной фазе: 25.10.2018(86) Заявка РСТ:  
CN 2017/077247 (20.03.2017)(87) Публикация заявки РСТ:  
WO 2017/162112 (28.09.2017)

Адрес для переписки:

129090, Москва, ул. Б. Спасская, 25, стр. 3, ООО  
"Юридическая фирма Городисский и  
Партнеры"

(71) Заявитель(и):

**АЛИБАБА ГРУП ХОЛДИНГ ЛИМИТЕД  
(КУ)**

(72) Автор(ы):

**МЭН Фэй (CN)****(54) СПОСОБ И УСТРОЙСТВО ДЛЯ РЕГИСТРАЦИИ ЛИЧНОСТИ****(57) Формула изобретения**

1. Способ регистрации личности, при этом способ содержит этапы, на которых: принимают, посредством терминального устройства, информацию о биометрическом признаке пользователя, которая подлежит подтверждению;

сопоставляют эталонную информацию о биометрическом признаке, согласующуюся с информацией о биометрическом признаке, которая подлежит подтверждению, в предварительно сохраненной информации о биометрическом признаке;

отыскивают закрытый ключ, соответствующий идентификатору, на основе идентификатора, соответствующего эталонной информации о биометрическом признаке, после того как сопоставление успешно выполняется; и

регистрируют личность пользователя с помощью сервера на основе информации о биометрическом признаке, которая подлежит подтверждению, когда закрытый ключ, соответствующий идентификатору, не идентифицируется, таким образом, сервер сохраняет открытый ключ, соответствующий информации о биометрическом признаке, которая подлежит подтверждению.

2. Способ по п. 1, в котором перед регистрацией личности пользователя с помощью сервера на основе информации о биометрическом признаке, которая подлежит подтверждению, способ дополнительно содержит этапы, на которых:

принимают пароль, введенный пользователем; и  
подтверждают, что пароль является корректным.

3. Способ по п. 1, в котором регистрация личности пользователя с помощью сервера на основе информации о биометрическом признаке, которая подлежит подтверждению, содержит этапы, на которых:

формируют закрытый ключ и открытый ключ, соответствующие идентификатору, на основе идентификатора, соответствующего эталонной информации о биометрическом признаке, которая совпадает с информацией о биометрическом признаке, которая подлежит подтверждению;

сохраняют сопоставляющее соотношение между идентификатором и сформированным закрытым ключом в терминальном устройстве; и

отправляют сопоставляющее соотношение между идентификатором и сформированным открытым ключом серверу для хранения.

4. Способ по п. 1, при этом после регистрации личности пользователя с помощью сервера способ дополнительно содержит этап, на котором:

отправляют запрос обработки службы серверу на основе информации о биометрическом признаке, которая подлежит подтверждению, таким образом, сервер выполняет обработку службы на основе открытого ключа, соответствующего информации о биометрическом признаке, которая подлежит подтверждению.

5. Способ по п. 4, в котором отправка запроса обработки службы серверу на основе информации о биометрическом признаке, которая должна быть подтверждена, содержит этапы, на которых:

подписывают служебную информацию на основе сформированного закрытого ключа и отправляют запрос обработки службы, который содержит подписанную служебную информацию и идентификатор, серверу, таким образом, сервер определяет открытый ключ, соответствующий идентификатору, содержащемуся в принятом запросе обработки службы, и выполняет обработку службы на основе определенного открытого ключа и подписанной служебной информации.

6. Способ по п. 4 или 5, в котором запрос обработки службы содержит запрос оплаты.

7. Устройство регистрации личности, при этом устройство содержит:

модуль приема, сконфигурированный, чтобы принимать информацию о биометрическом признаке пользователя, которая подлежит подтверждению;

модуль сопоставления, сконфигурированный, чтобы сопоставлять эталонную информацию о биометрическом признаке, согласующуюся с информацией о биометрическом признаке, которая подлежит подтверждению, в предварительно сохраненной информации о биометрическом признаке;

модуль поиска, сконфигурированный, чтобы искать закрытый ключ, соответствующий идентификатору, на основе идентификатора, соответствующего эталонной информации о биометрическом признаке, после того как сопоставление успешно выполняется; и

модуль регистрации, сконфигурированный, чтобы регистрировать личность пользователя с помощью сервера на основе информации о биометрическом признаке, которая подлежит подтверждению, когда модуль поиска не идентифицирует закрытый ключ, соответствующий идентификатору, таким образом, сервер сохраняет открытый ключ, соответствующий информации о биометрическом признаке, которая подлежит подтверждению.

8. Устройство по п. 7, при этом устройство дополнительно содержит:

модуль подтверждения пароля, сконфигурированный, чтобы принимать пароль, введенный пользователем, и подтверждать, что пароль является корректным, прежде чем модуль регистрации регистрирует личность пользователя с помощью сервера на основе информации о биометрическом признаке, которая подлежит подтверждению.

9. Устройство по п. 7, в котором модуль регистрации конфигурируется, чтобы

формировать закрытый ключ и открытый ключ, соответствующие идентификатору, на основе идентификатора, соответствующего эталонной информации о биометрическом признаке, которая совпадает с информацией о биометрическом признаке, которая подлежит подтверждению; сохранять сопоставляющее соотношение между идентификатором и сформированным закрытым ключом в терминальном устройстве; и отправлять сопоставляющее соотношение между идентификатором и сформированным открытым ключом серверу для хранения.

10. Устройство по п. 7, при этом устройство дополнительно содержит:

модуль обработки, сконфигурированный, чтобы отправлять запрос обработки службы серверу на основе информации о биометрическом признаке, которая подлежит подтверждению, после того как модуль регистрации регистрирует личность пользователя с помощью сервера, таким образом, сервер выполняет обработку службы на основе открытого ключа, соответствующего информации о биометрическом признаке, которая подлежит подтверждению.

11. Устройство по п. 10, в котором модуль обработки конфигурируется, чтобы подписывать служебную информацию на основе сформированного закрытого ключа и отправлять запрос обработки службы, который содержит подписанную служебную информацию и идентификатор, серверу, таким образом, сервер определяет открытый ключ, соответствующий идентификатору, содержащемуся в принятом запросе обработки службы, и выполняет обработку службы на основе определенного открытого ключа и подписанной служебной информации.

12. Устройство по п. 10 или 11, в котором запрос обработки службы содержит запрос оплаты.

А 2 0 1 8 1 3 7 4 8 7  
R U

R U 2 0 1 8 1 3 7 4 8 7  
A