конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто'2024»

О некоторых системах подтверждения ПДн без их разглашения, использующих неклассические криптографические механизмы

Кяжин Сергей Николаевич, к.ф.-м.н., НТЦ ЦК, НИЯУ МИФИ, КриптоПро
Утехина Мария, студент МГУ им. М.В. Ломоносова, стажер-исследователь НТЦ ЦК
Зюзин Юрий, студент МГУ им. М.В. Ломоносова, стажер-исследователь НТЦ ЦК
Махонин Илья, студент НИЯУ МИФИ, стажер-аналитик НТЦ ЦК
Лебедев Вадим, студент НИЯУ МИФИ, стажер-аналитик НТЦ ЦК

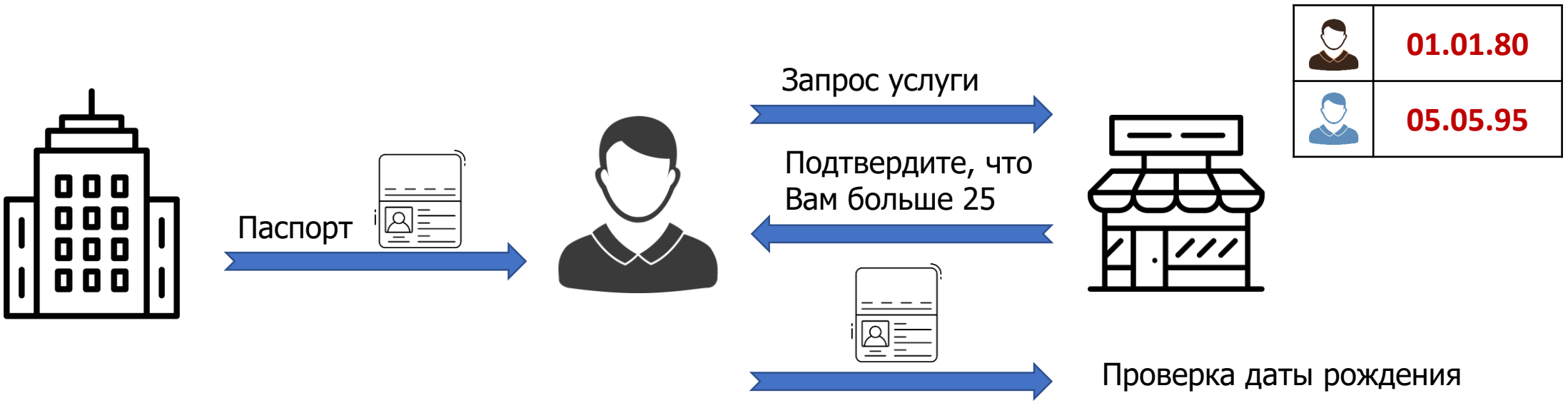
Работа выполнена в рамках научно-исследовательского и аналитического сопровождения работ АНО «НТЦ ЦК»

Подтверждение ПДн

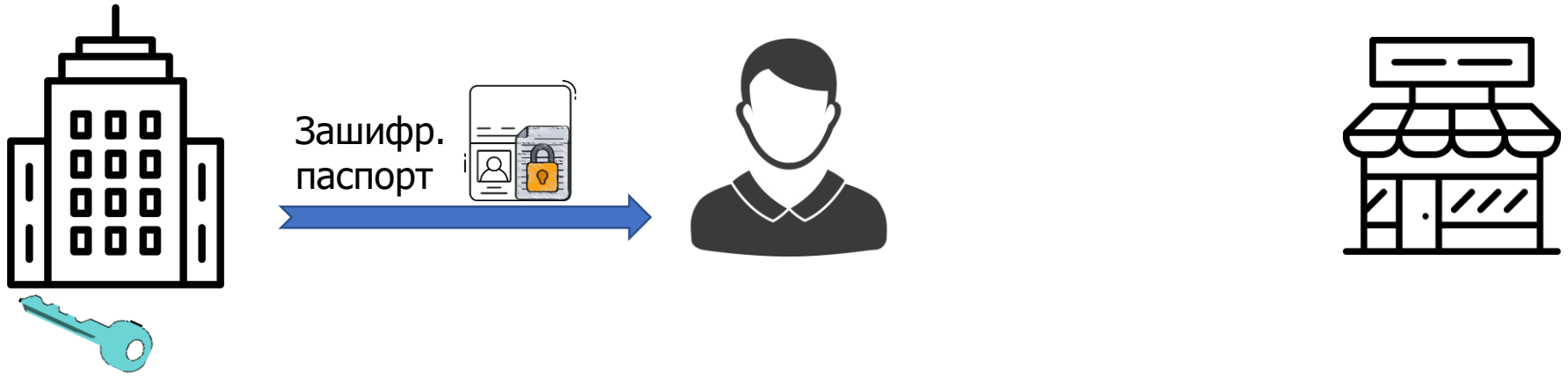
=
- ФИО
- Дата рождения
- Место рождения
- Место жительства
- …

Подтверждение ПДн

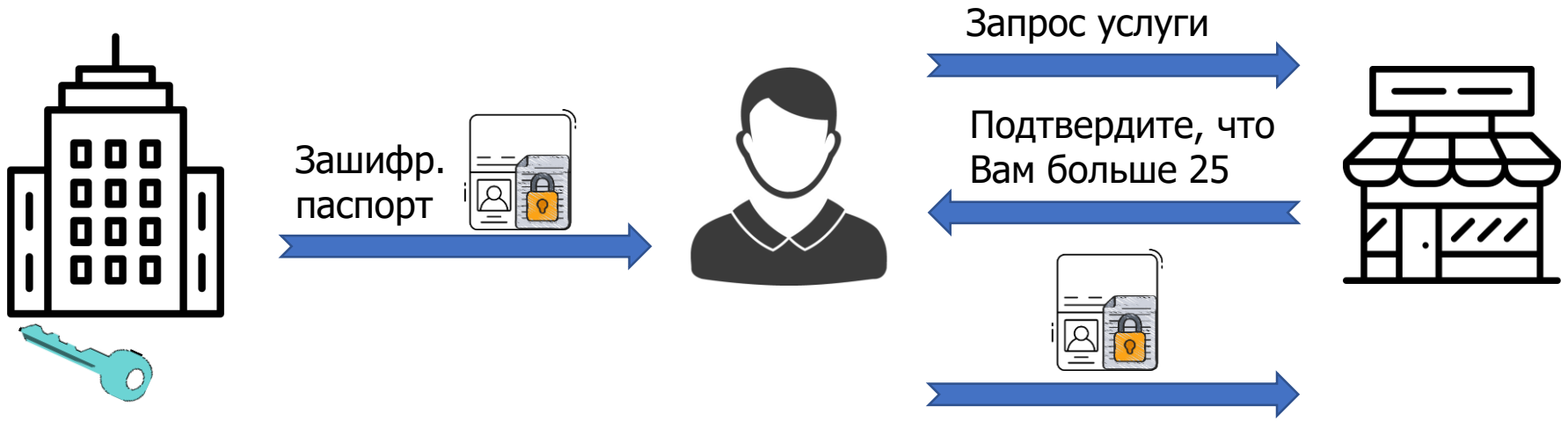
Подтверждение ПДн



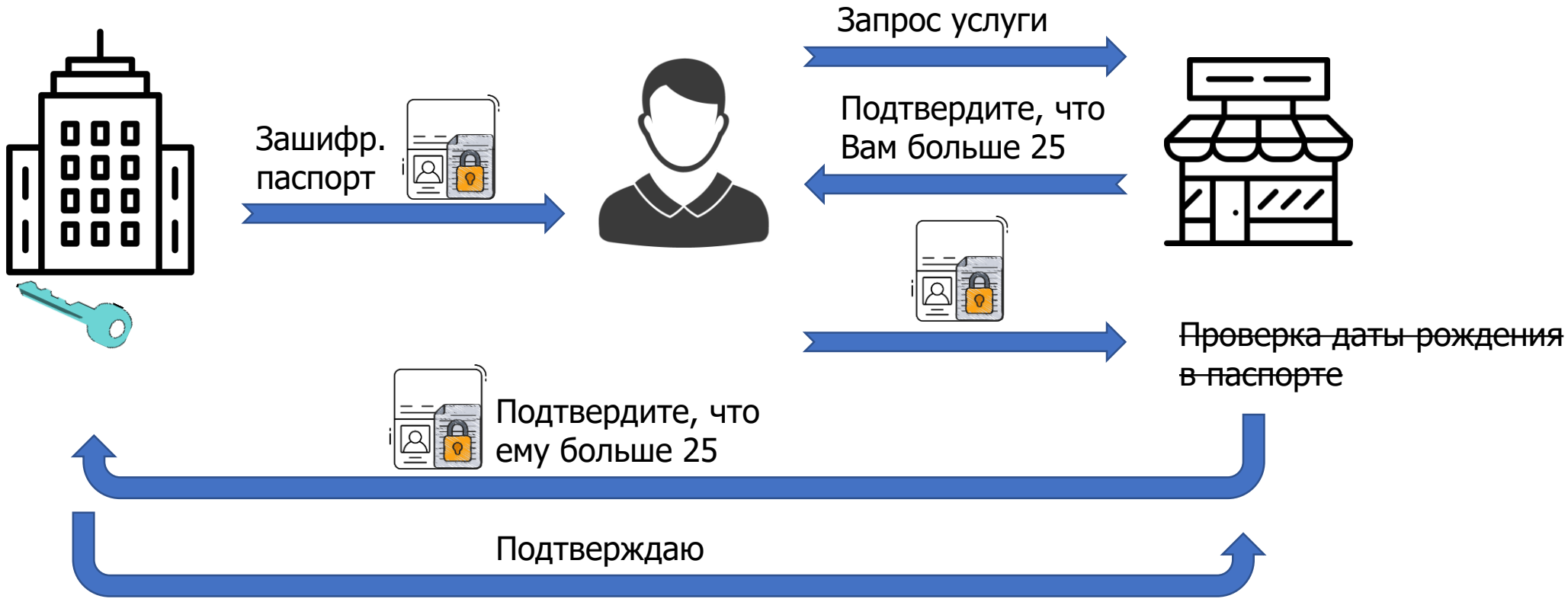
Подтверждение ПДн без их разглашения



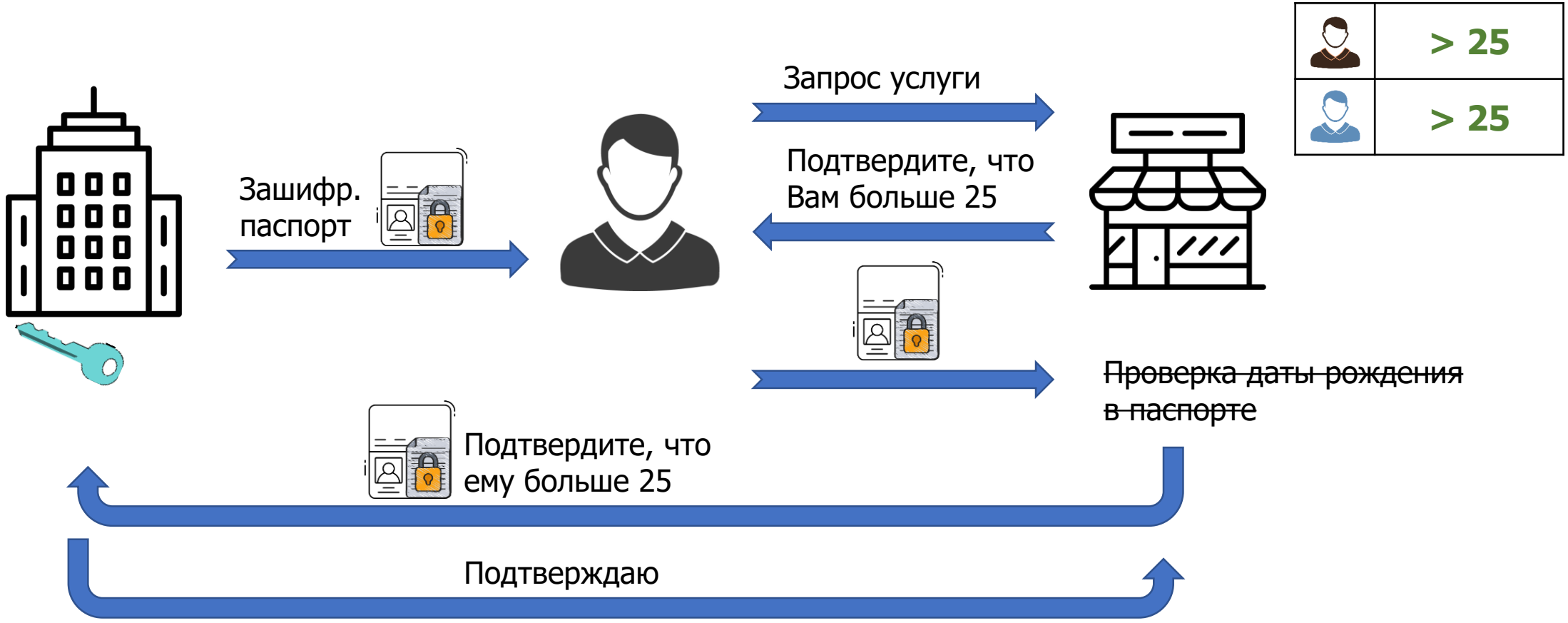
Подтверждение ПДн без их разглашения



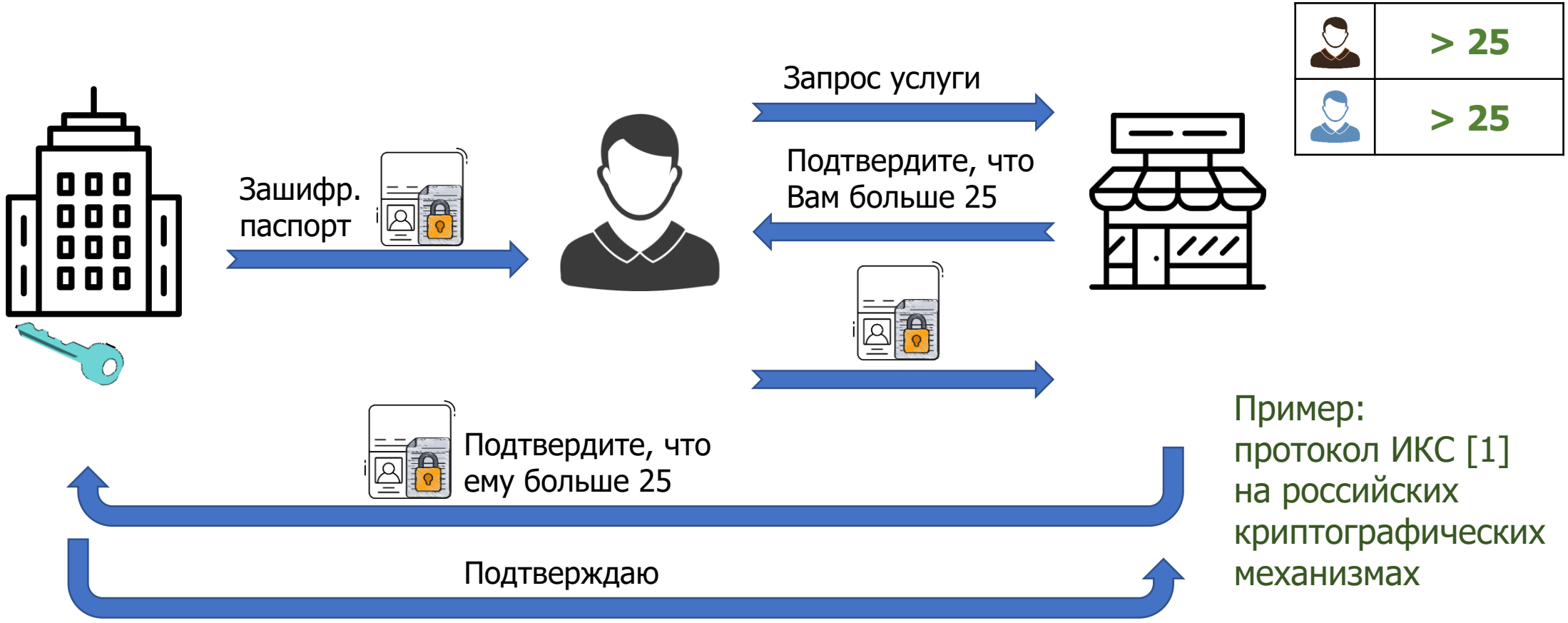
Подтверждение ПДн без их разглашения



Подтверждение ПДн без их разглашения



Подтверждение ПДн без их разглашения

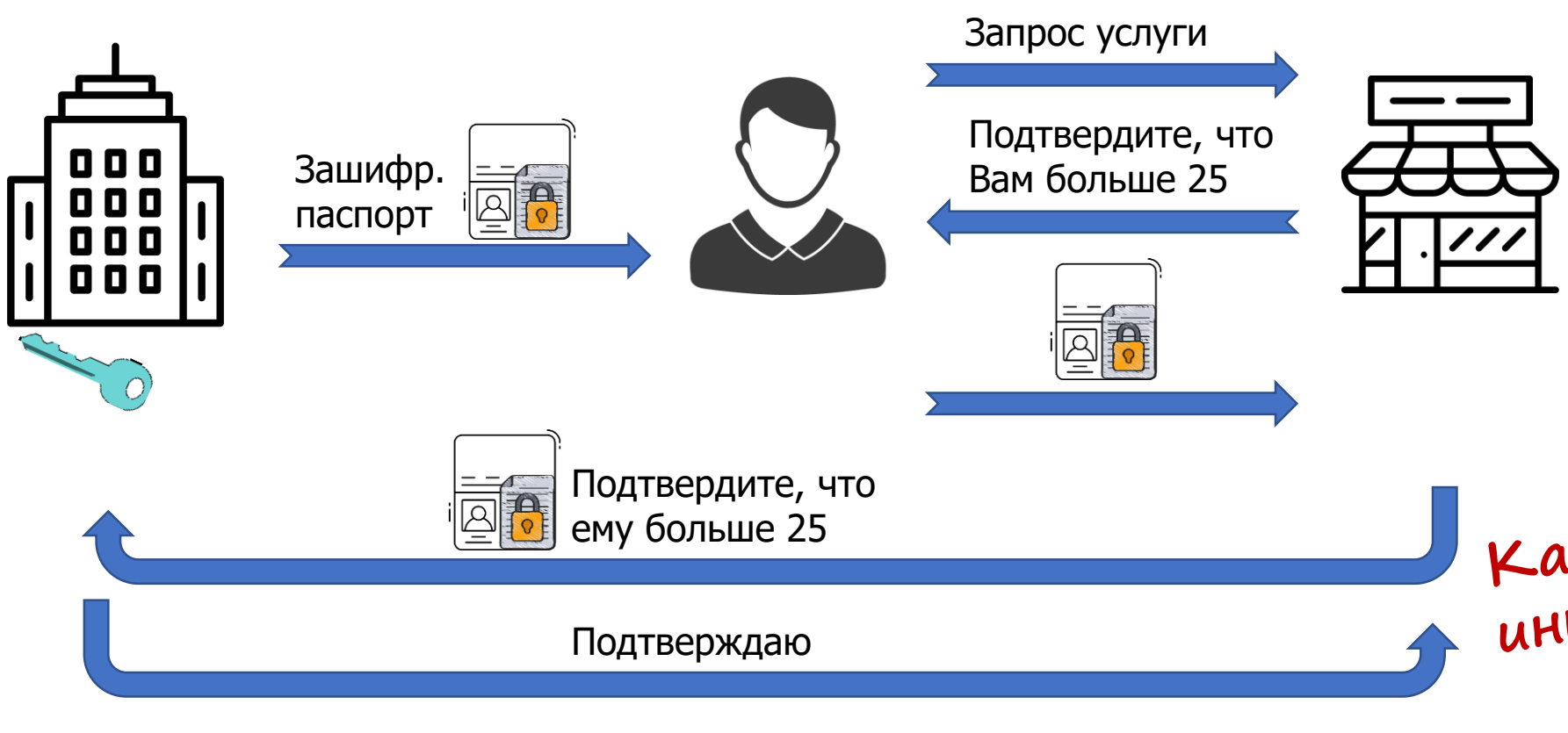


Пример:
протокол ИКС [1]
на российских
криптографических
механизмах

[1] Бельский В.С., Герасимов И.Ю., Царегородцев К.Д., Чижов И.В. Протокол обмена персональными данными: ИКС // International Journal of Open Information Technologies. 2020. Т. 8, № 6, с. 1–23

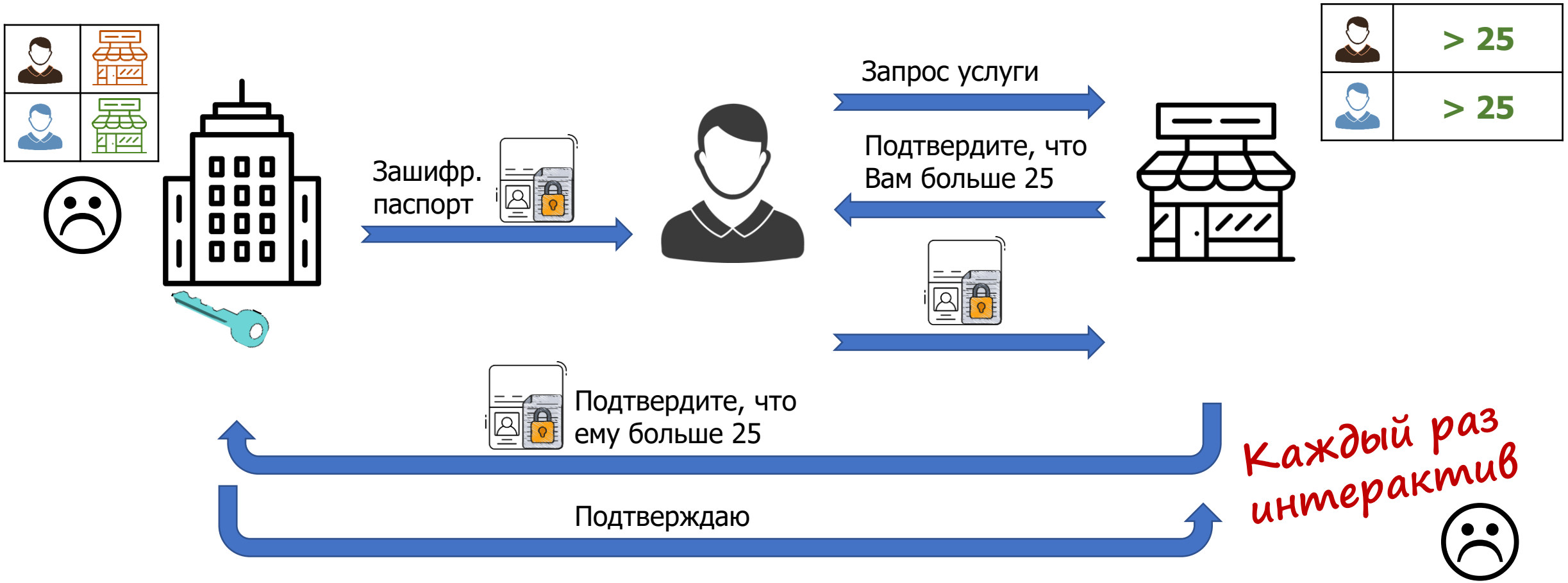
Подтверждение ПДн без их разглашения

	> 25
	> 25

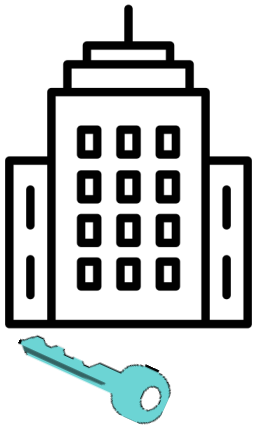


Каждый раз интерактив

Подтверждение ПДн без их разглашения



Подтверждение ПДн без их разглашения



Зашифр. паспорт

Запрос услуги

Подтвердите, что Вам больше 25

Подтвердите, что ему больше 25

Подтверждаю

Каждый раз интерактив

Архитектура взаимодействия «желаемой» системы

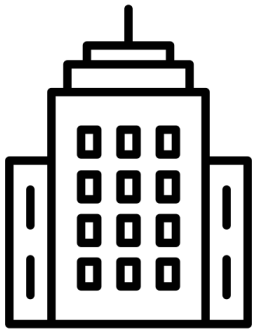
Клиент

Атрибуты

- ФИО
- Дата рождения
- Место рождения
- Место жительства
- …

Архитектура взаимодействия «желаемой» системы

Эмитент **Клиент**



Выпуск токена

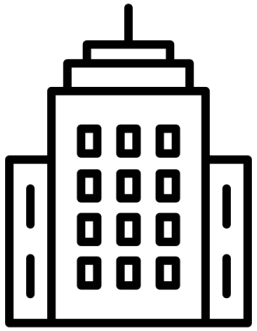
= **токен** для атрибутов

- ФИО
- Дата рождения
- Место рождения
- Место жительства
- …

Архитектура взаимодействия «желаемой» системы

Эмитент

Клиент

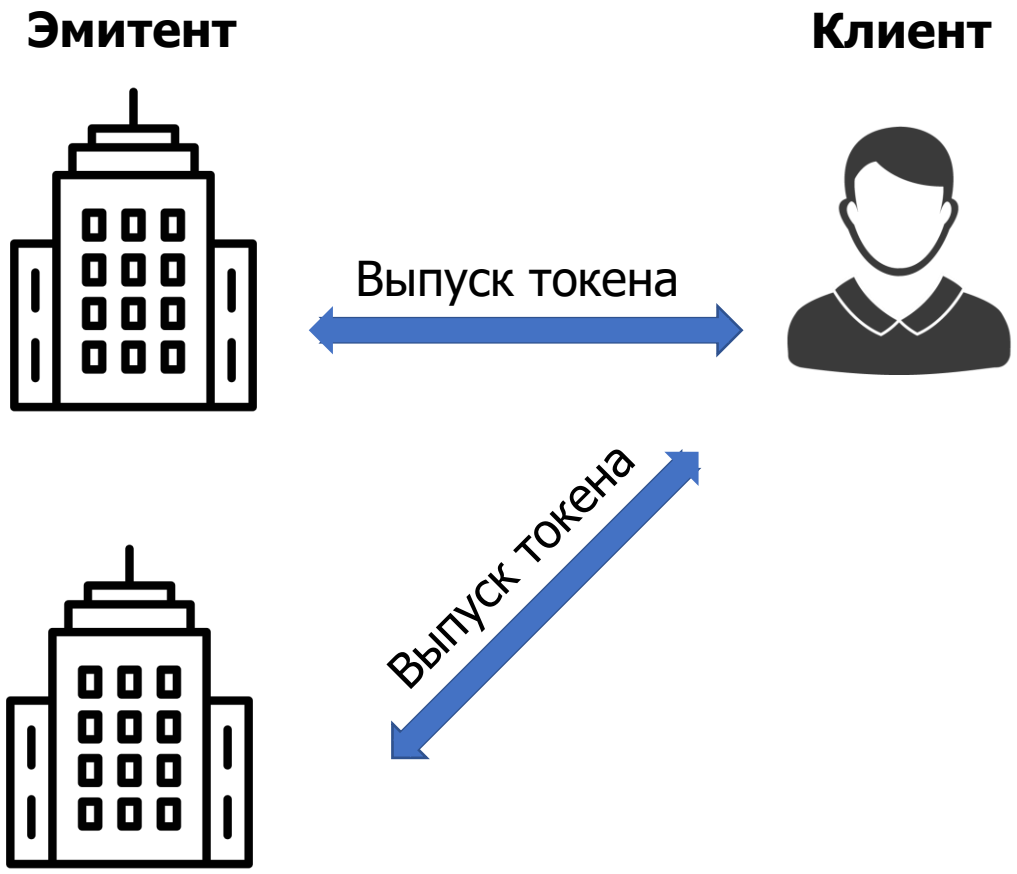


Выпуск токена

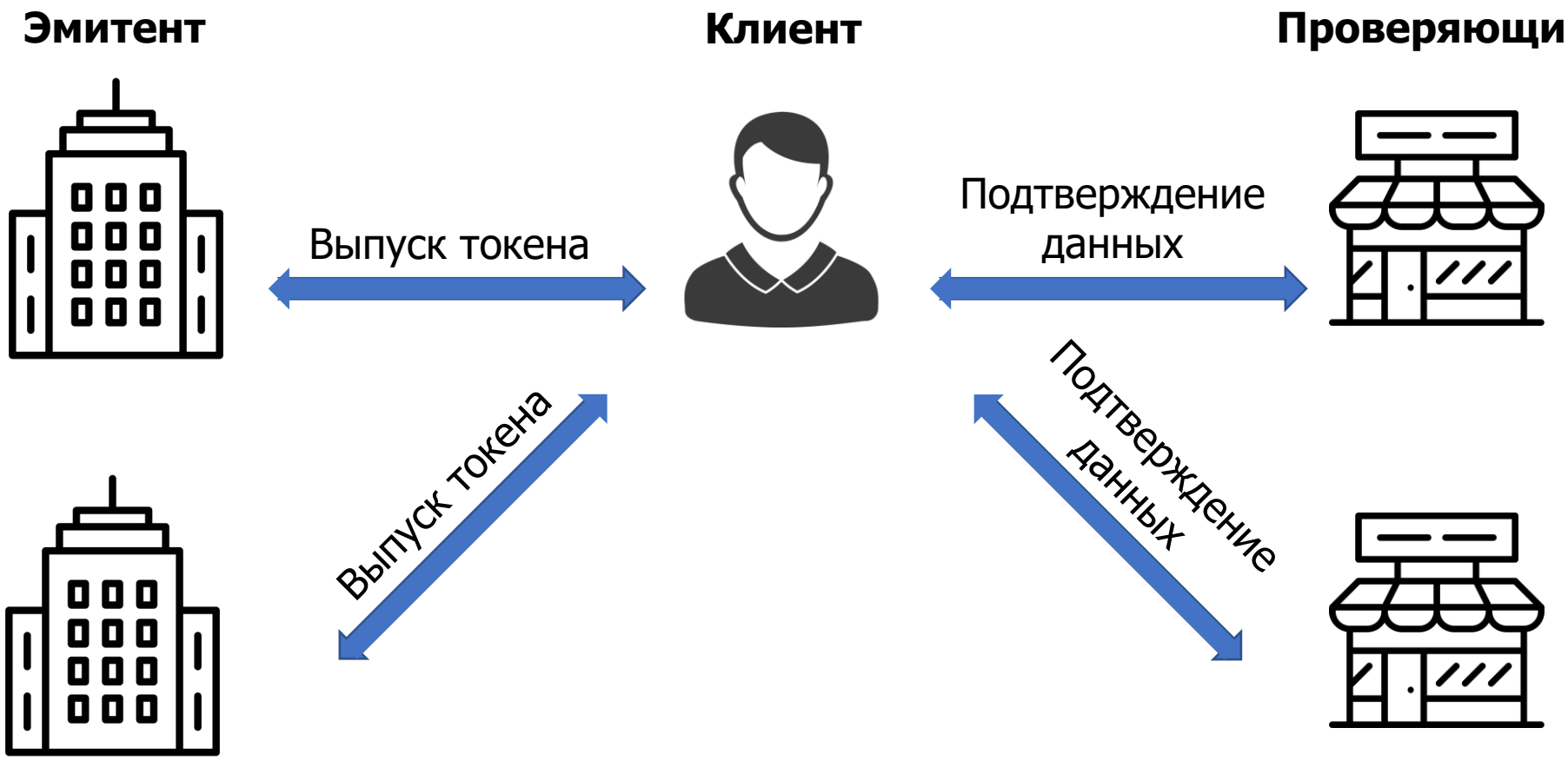
= **токен** для атрибутов

- ФИО
- Дата рождения
- Место рождения
- Место жительства
- …

Архитектура взаимодействия «желаемой» системы

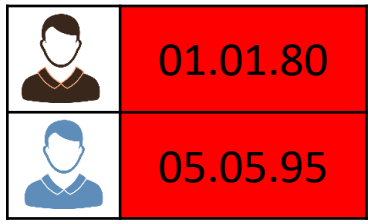


Архитектура взаимодействия «желаемой» системы



Желаемые свойства безопасности

Конфиденциальность атрибутов

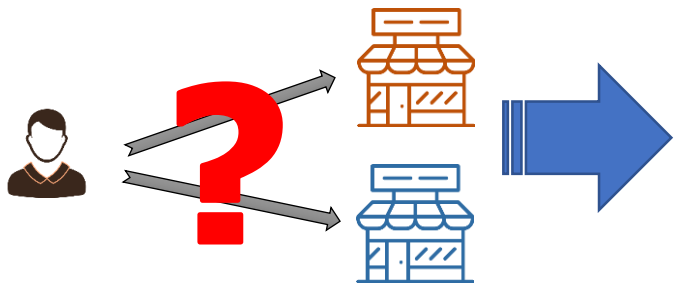


Неподделываемость токена

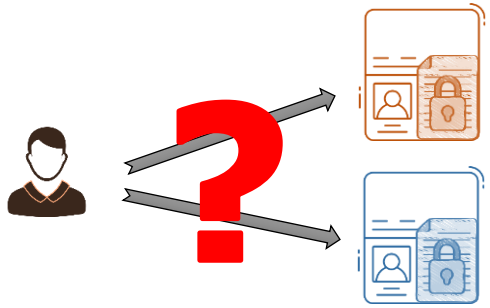
Основные

Дополнительные

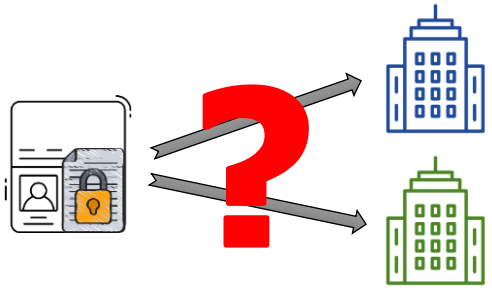
Анонимность обслуживания



Несвязываемость токенов



Несвязываемость эмитентов



Системы Anonymous Credentials

Пример таблицы из обзорной статьи [2]

	Category	Assumptions	Selective disclosure	Delegatable	Issuer-hiding	Updatable	Issuer/Verifier Combo	Credential Size	Prove Complexity	Verify Complexity	Implemented
U-Prove [76]		DLog	✓	•	•	•	•	$(\ell{+}4)\mathbb{G} + (\ell+2)\mathbb{Z}_p$	$(\ell{+}5)$e	$(5\ell{+}6)$e	✓
idemix [34]	ZK	SRSA	✓	•	•	•	•	$3\mathbb{Z}_N + \pi$	$3\text{e} + \pi_p$	π_v	✓
CL04 [32]	ZK	LRSW, DDH	✓	•	•	•	•	$(2\ell{+}3)\mathbb{G}$	$(2\ell{+}3)$e	$(\ell+1)\text{e} + 3\text{p}$	
BCC+09 [10]	ZK	HSDH, CDH	•	✓	•	•	•	$\ell \cdot \pi$	$(2\ell \cdot \lvert\pi\rvert)$e	$(\ell \cdot \lvert\pi\rvert)$p	
PCS [63]	ZK	q-DHE, CDH	✓	•	•	•	•	$(\ell\ {+}5)\mathbb{G}$	$(2\ell + N{+}5)$e	$(2\ell+3)$p	✓
BB18 [17]	ZK	GGM	✓	✓	•	•	•	$(\ell{+}2)\mathbb{G} + \pi$	$(\ell{+}1)\text{e} + \pi_p$	π_v	
BEKRS21 [19]	ZK	NIZK + Sig	✓	•	✓	•	✗	–	–	–	–
BBDE19 [18]	ZK	Blind Sig	•	•	•	✓	•	–	–	–	–
CMZ14 [36]	ZK	DDH, q-SDH	✓	•	✗	•	✓	$(\ell{+}5)\mathbb{G} + \pi$	$(4\ell+4)$e	$(2\ell+2)$e	✓
CPZ20 [37]	ZK	DDH	✓	•	✗	•	✓	$(\ell{+}3)\mathbb{G} + \pi$	$(\ell+4)$e	ℓp	✓
Verheul [88]	SB	DDH	•	•	•	•	✗	–	–	–	–
RVH17 [78]	SB	whLRSW	✓	•	•	•	✗	$(\ell+4)\mathbb{G}$	$(2\ell+7)$e	$(3\ell+1)\text{e} + 4$	
PO19 [77]	SB	DDH, SXDH	✓	✓	•	•	✗	$6\mathbb{G}{+}\ell\mathbb{Z}_p$	$(\ell+1)$e	$(\ell+2)$e	
CL20 [44]	SB	ABDDH+, GGM	•	✓	•	•	✗	–	–	–	–
CLP22 [42]	SB	XKerMDH	✓	•	✓	•	✗	$32\ \mathbb{G} + 4\ \mathbb{Z}_p$	19p	17p	
BMMS22 [73]	SB	DDH, GGM	✓	✓	•	•	✗	$5\ \mathbb{G} + \ell \cdot C$	$\ell \cdot C_t + \pi_p$	π_v	

KVAC

[2] Kakvi S.A., *et al.* SoK: Anonymous Credentials // Security Standardisation Research. SSR 2023. LNCS, vol. 13895. Springer, Cham, 2023, pp. 129–151.

Системы Anonymous Credentials

	Криптографическое «ядро»	**Атрибуты**	**Доказываемые утверждения**
U-Prove			
Idemix			
ePCS			
Privacy Pass			
Nymble			

[U-Prove] Paquin C., Zaverucha G. U-Prove Cryptographic Specification. V. 1.1. Microsoft Corporation. 2013. https://www.microsoft.com/en-us/research/publication/u-prove-cryptographic-specification-v1-1-revision-3/.
[Idemix] Specification of the Identity Mixer Cryptographic Library. Version 2.3.0. IBM Research, 2010. https://dominoweb.draco.res.ibm.com/reports/rz3730_revised.pdf
[ePCS] Kaaniche N., *et al.* Anonymous certification for E-assessment opinion polls // Journal of Ambient Intelligence and Humanized Computing. 2023, No. 14.
[Privacy Pass] Privacy Pass. A privacy-enhancing protocol and browser extension. https://privacypass.github.io/.
[Nymble] Nymble: Anonymous IP-Address Blocking. https://cgi.luddy.indiana.edu/~kapadia/nymble/

Системы Anonymous Credentials

	Криптографическое «ядро»	**Атрибуты**	**Доказываемые утверждения**
U-Prove			
Idemix			
ePCS			
Privacy Pass	KVAC		
Nymble			

Системы типа KVAC

Не подходит для целевого сценария

Системы Anonymous Credentials

	Криптографическое «ядро»	**Атрибуты**	**Доказываемые утверждения**
U-Prove			
Idemix			
ePCS			
Privacy Pass	KVAC	Нет	Наличие токена ☺
Nymble			

Системы Anonymous Credentials

	Криптографическое «ядро»	**Атрибуты**	**Доказываемые утверждения**
U-Prove	Подпись вслепую + ZKP		
Idemix			
ePCS			
Privacy Pass	KVAC	Нет	Наличие токена ☺
Nymble			

Системы U-Prove и Idemix

Системы Anonymous Credentials

<table>
<tr><th></th><th>Криптографическое «ядро»</th><th>Атрибуты</th><th>Доказываемые утверждения</th></tr>
<tr><td>U-Prove</td><td rowspan="2">Подпись вслепую + ZKP</td><td rowspan="2">Битовые строки</td><td>Линейные функции + больше/меньше</td></tr>
<tr><td>Idemix</td><td>Больше/меньше константы</td></tr>
<tr><td>ePCS</td><td></td><td></td><td></td></tr>
<tr><td>Privacy Pass</td><td rowspan="2">KVAC</td><td rowspan="2">Нет</td><td rowspan="2">Наличие токена ☺</td></tr>
<tr><td>Nymble</td></tr>
</table>

Системы Anonymous Credentials

	Криптографическое «ядро»	**Атрибуты**	**Доказываемые утверждения**
U-Prove	Brands signature + «проприетарный» протокол ZKP	Битовые строки	Линейные функции + больше/меньше
Idemix	Camenisch-Lysyanskaya signature + «проприетарный» протокол ZKP		Больше/меньше константы
ePCS			
Privacy Pass	KVAC	Нет	Наличие токена ☺
Nymble			

Системы Anonymous Credentials

	Криптографическое «ядро»	**Атрибуты**	**Доказываемые утверждения**
U-Prove	Brands signature + «проприетарный» протокол ZKP	Битовые строки	Линейные функции + больше/меньше
Idemix	Camenisch-Lysyanskaya signature + «проприетарный» протокол ZKP		Больше/меньше константы
ePCS	Attribute based signature	0/1	Булевы функции
Privacy Pass	KVAC	Нет	Наличие токена ☺
Nymble			