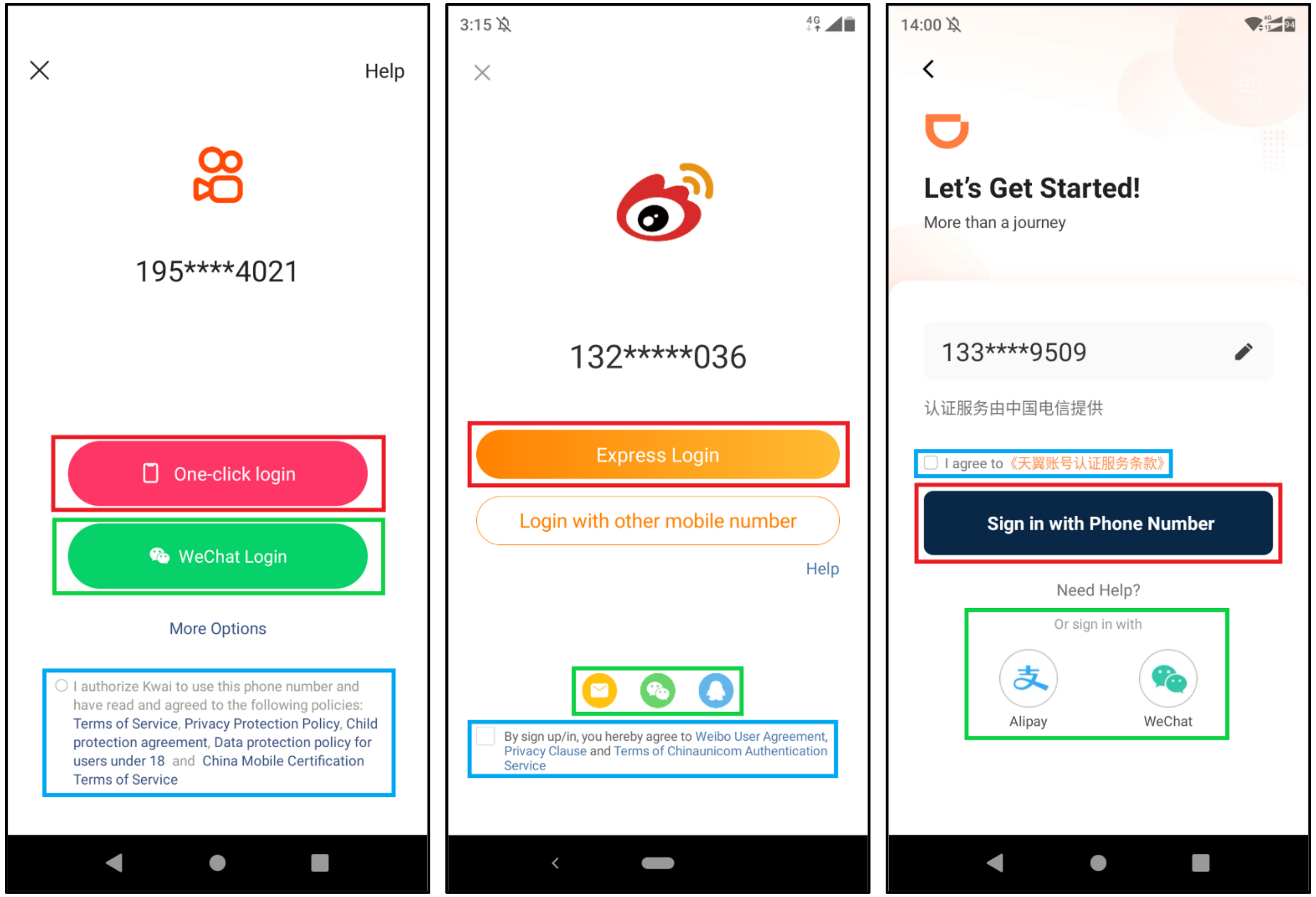
SIMulation: Demystifying (Insecure) Cellular Network based One-Tap Authentication Services

Ziyi Zhou[1], Xing Han[2], Zeyuan Chen[1], Yuhong Nan[3], Juanru Li[1] and Dawu Gu[1]

[1]Shanghai Jiao Tong University, Shanghai, China
[2]University of Electronic Science and Technology of China, Chengdu, China
[3]Sun Yat-sen University, Guangzhou, China

One-Tap Authentication (OTAuth) Scheme



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

□ By sign up/in, you hereby agree to Weibo User Agreement, Privacy Clause and Terms of Chinaunicom Authentication Service

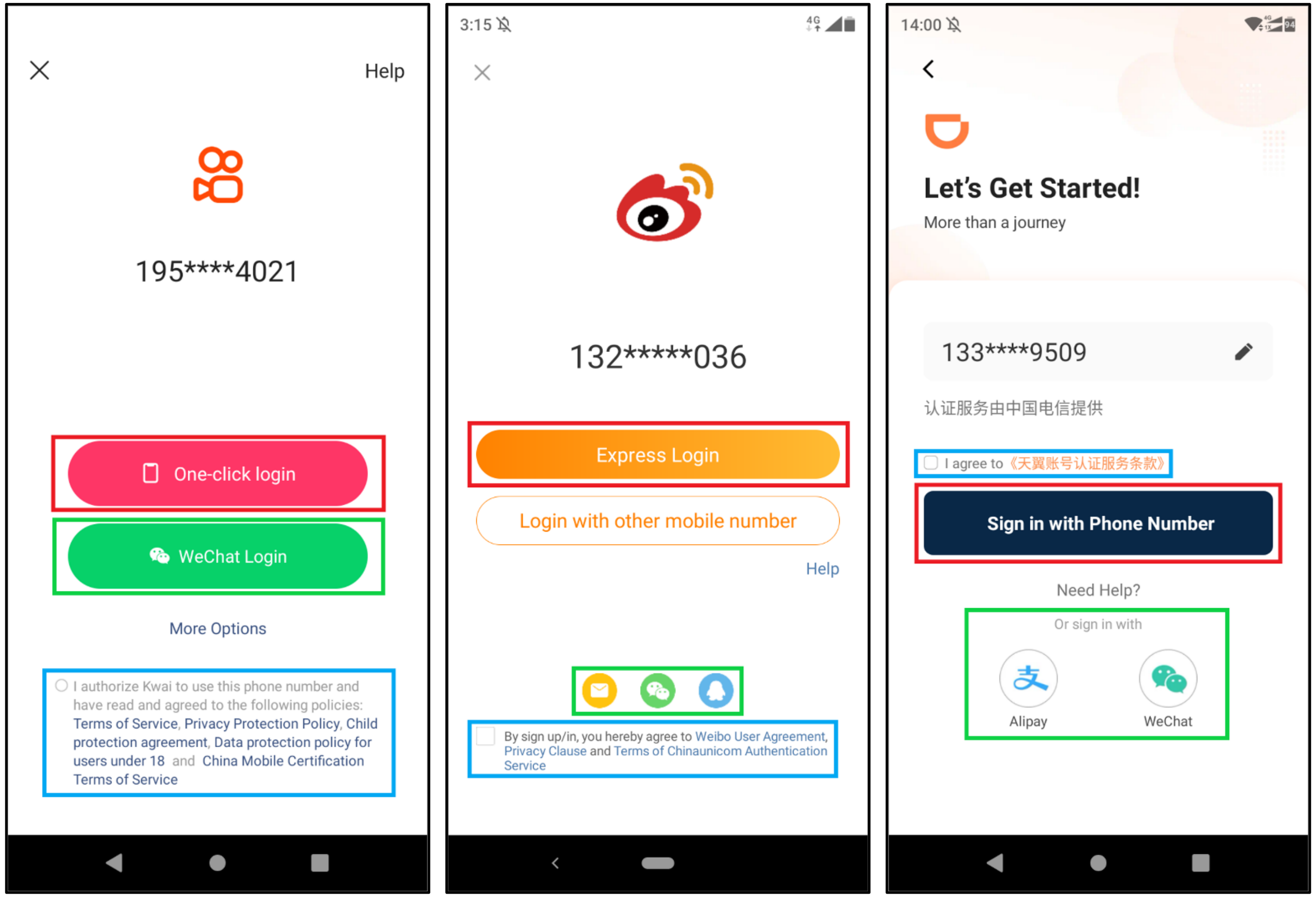
认证服务由中国电信提供

□ I agree to《天翼账号认证服务条款》

(a) China Mobile (b) China Unicom (c) China Telecom

Typical OTAuth services of different Mobile Network Operators (MNOs)

One-Tap Authentication (OTAuth) Scheme



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

□ By sign up/in, you hereby agree to Weibo User Agreement, Privacy Clause and Terms of Chinaunicom Authentication Service

认证服务由中国电信提供

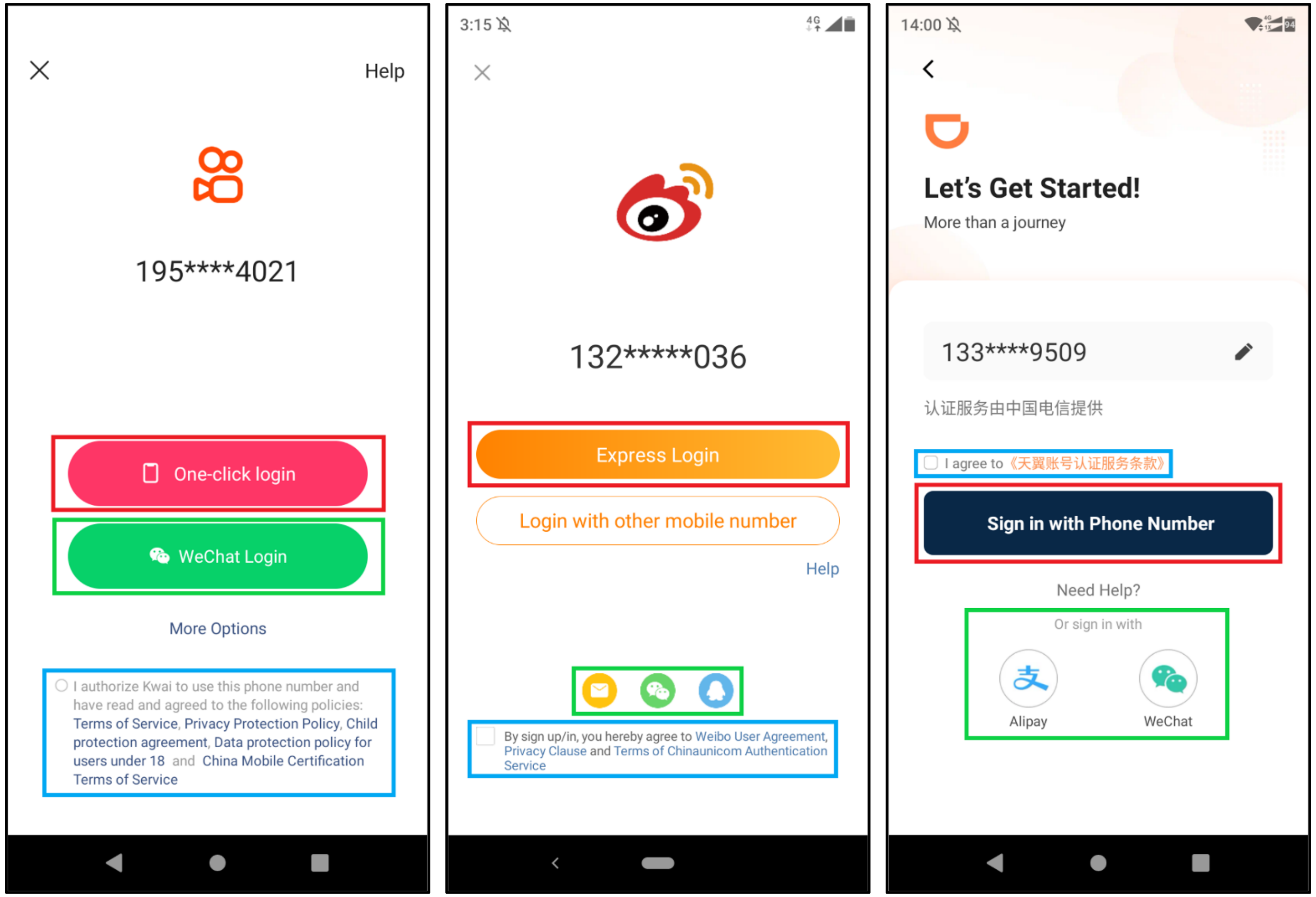
□ I agree to《天翼账号认证服务条款》

(a) China Mobile (b) China Unicom (c) China Telecom

Typical OTAuth services of different Mobile Network Operators (MNOs)

- **Log in to user's app account with the local phone number**

One-Tap Authentication (OTAuth) Scheme



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

132*****036

□ By sign up/in, you hereby agree to Weibo User Agreement, Privacy Clause and Terms of Chinaunicom Authentication Service

Let’s Get Started!

More than a journey

认证服务由中国电信提供

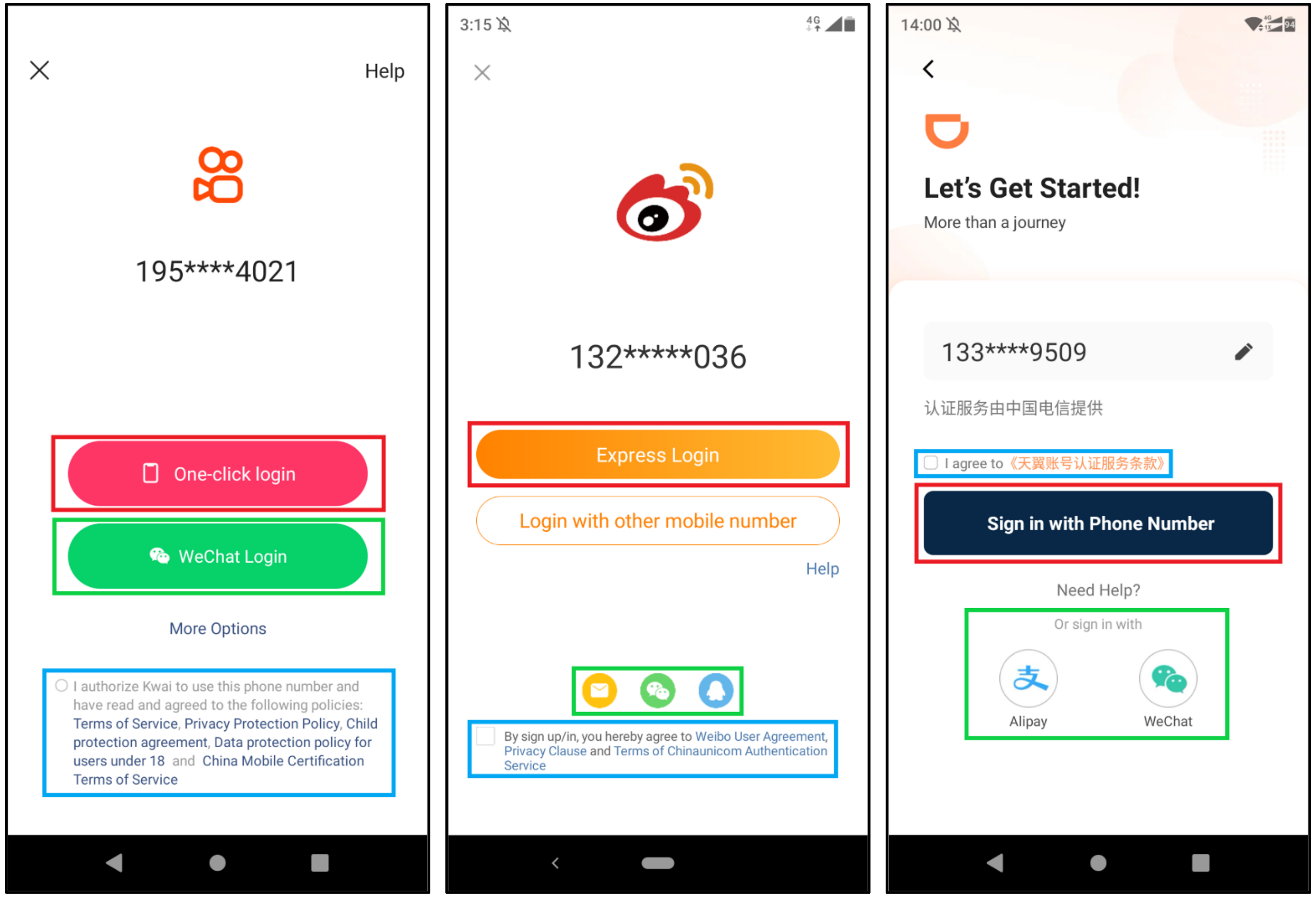
□ I agree to《天翼账号认证服务条款》

(a) China Mobile (b) China Unicom (c) China Telecom

Typical OTAuth services of different Mobile Network Operators (MNOs)

- **Log in to user's app account with the local phone number**
- **Only need one tap on the screen**

One-Tap Authentication (OTAuth) Scheme



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

□ By sign up/in, you hereby agree to Weibo User Agreement, Privacy Clause and Terms of Chinaunicom Authentication Service

认证服务由中国电信提供

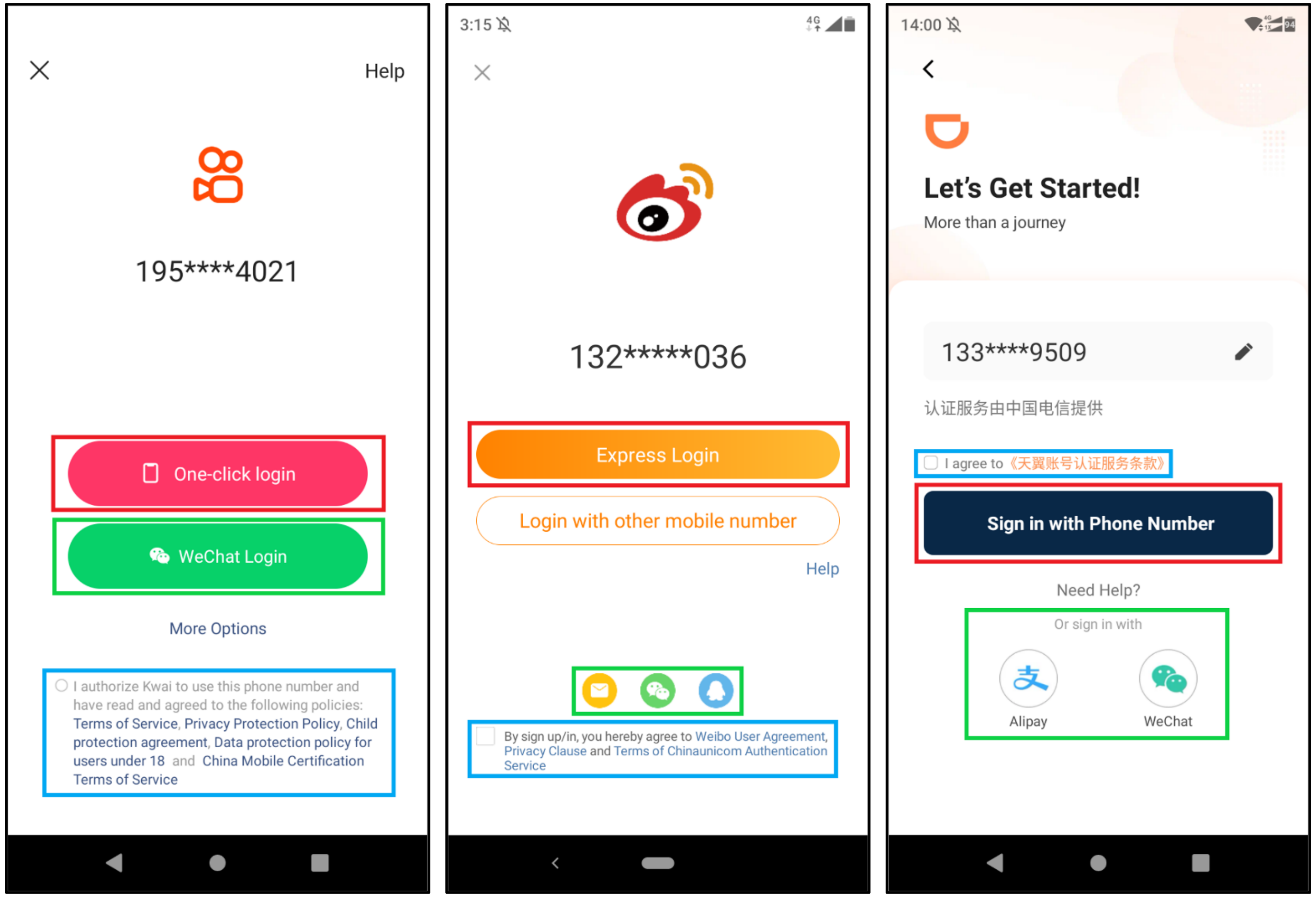
□ I agree to《天翼账号认证服务条款》

(a) China Mobile (b) China Unicom (c) China Telecom

Typical OTAuth services of different Mobile Network Operators (MNOs)

- **Log in to user's app account with the local phone number**
- **Only need one tap on the screen**
- **Without typing or pasting anything (e.g., SMS One-Time-Password)**

One-Tap Authentication (OTAuth) Scheme



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

□ By sign up/in, you hereby agree to Weibo User Agreement, Privacy Clause and Terms of Chinaunicom Authentication Service

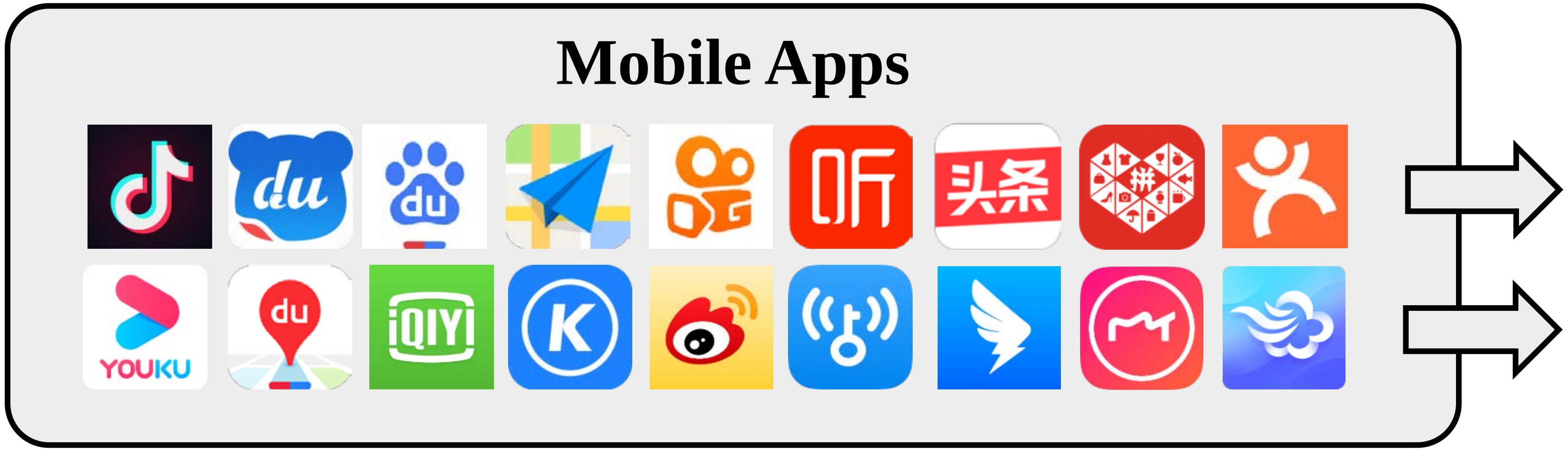
□ I agree to《天翼账号认证服务条款》

(a) China Mobile (b) China Unicom (c) China Telecom

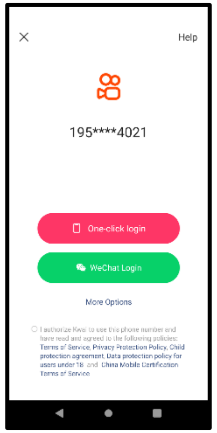
Typical OTAuth services of different Mobile Network Operators (MNOs)

- **Log in to user's app account with the local phone number**
- **Only need one tap on the screen**
- **Without typing or pasting anything (e.g., SMS One-Time-Password)**
- **Without remembering anything (e.g., username and password)**

OTAuth Services supported by MNOs

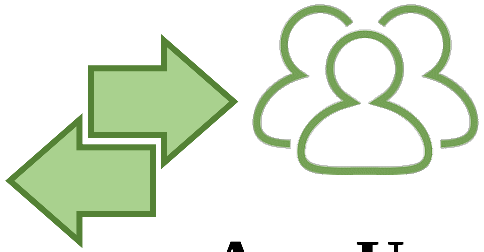

Mobile Apps

UI

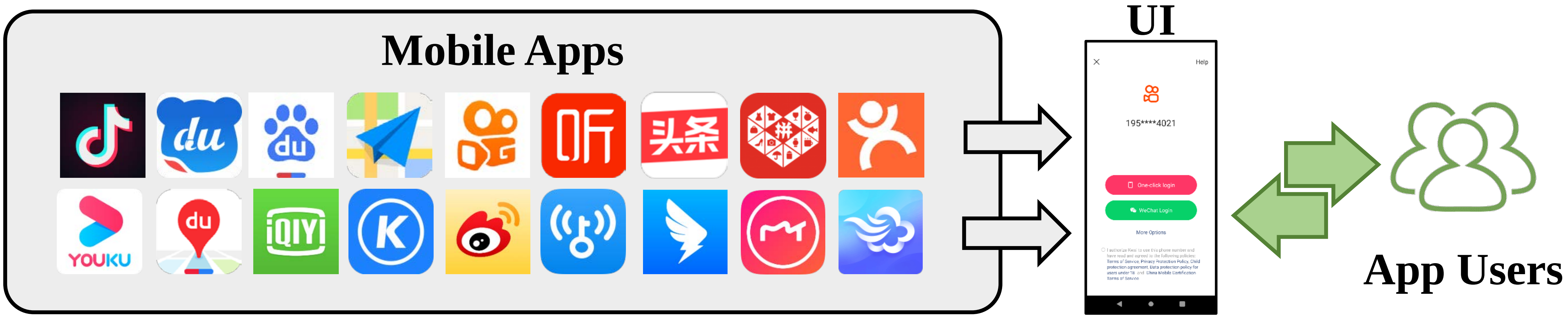


195****4021

○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service


App Users

OTAuth Services supported by MNOs



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

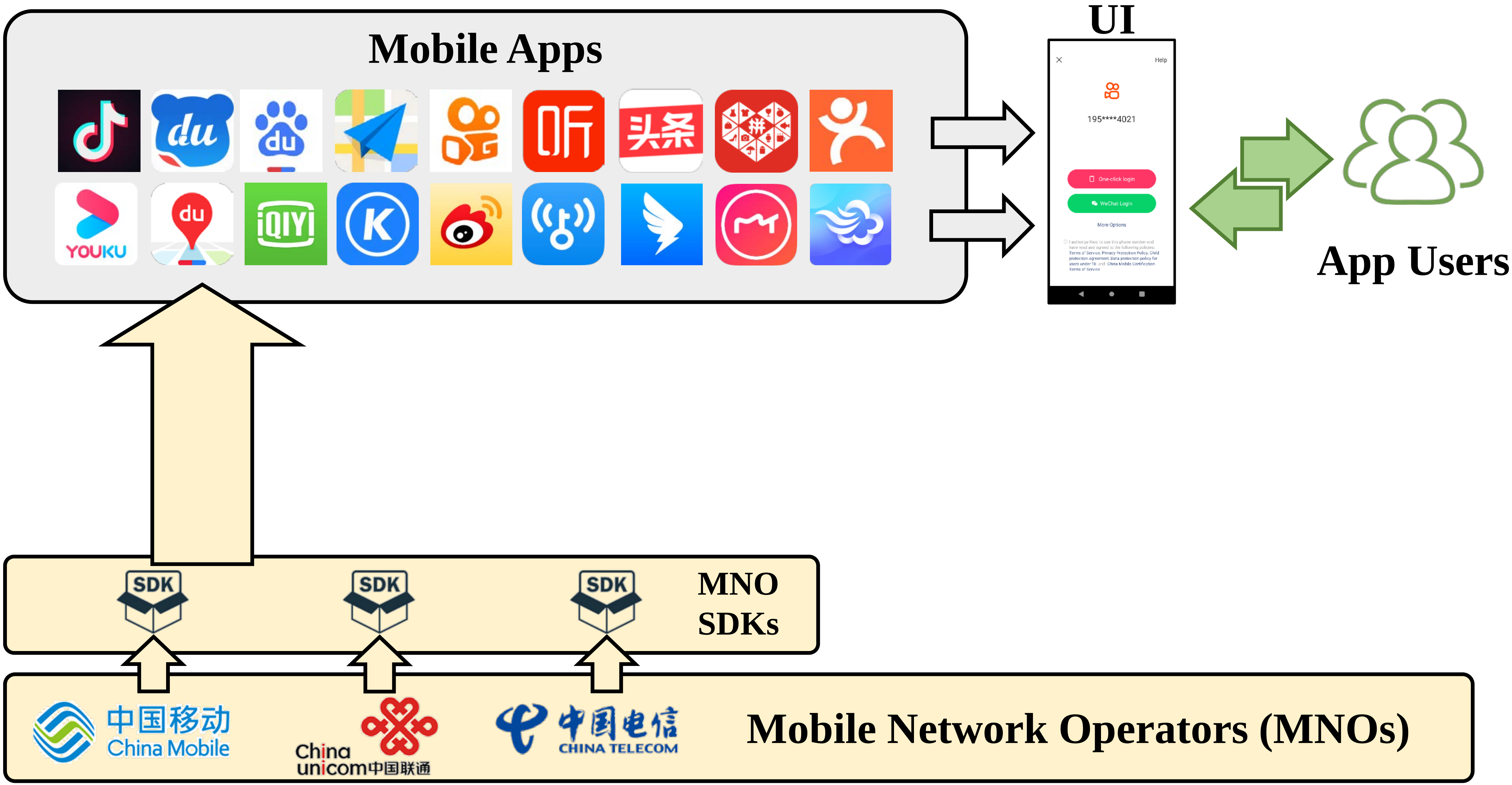
中国移动 China Mobile

China unicom中国联通

中国电信 CHINA TELECOM

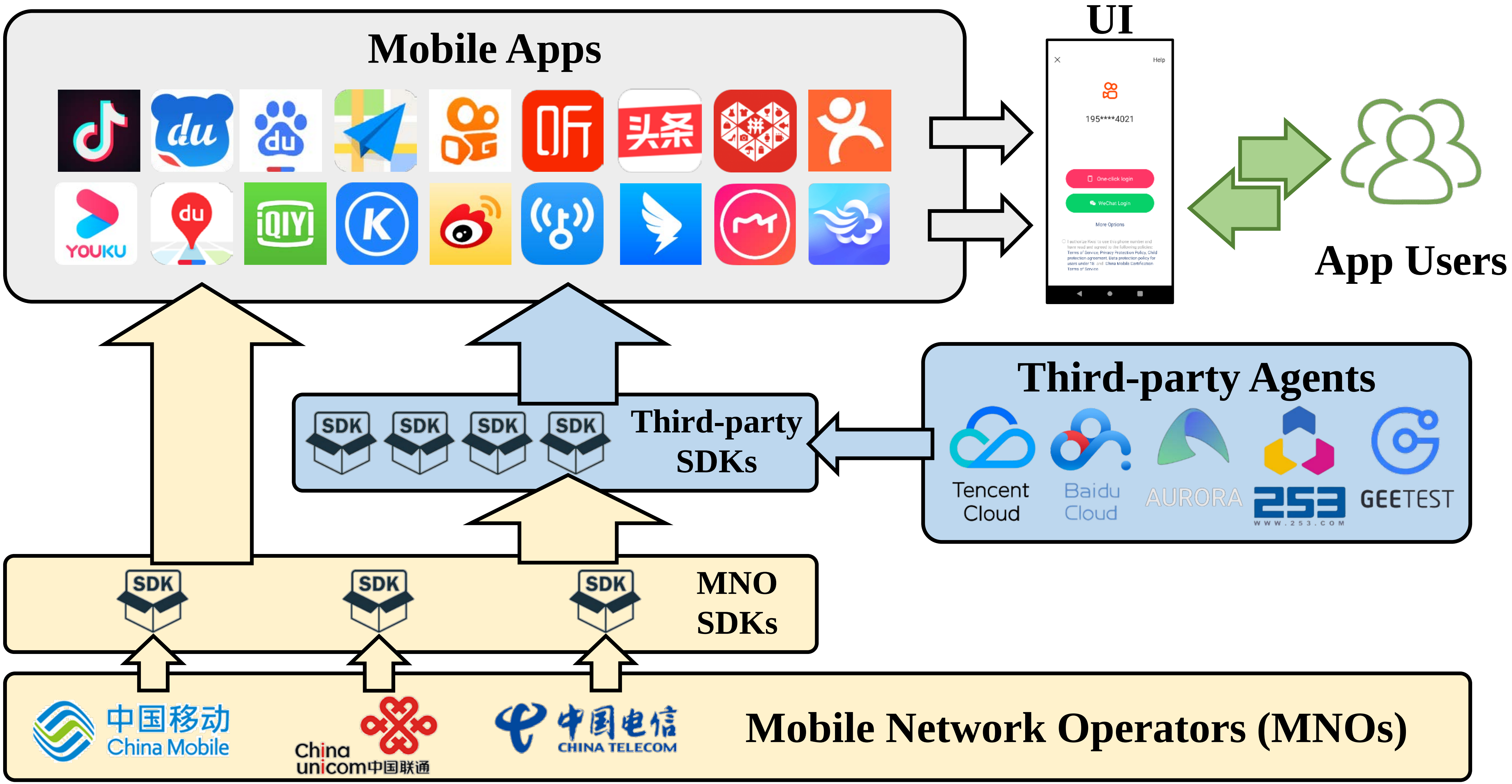
Mobile Network Operators (MNOs)

OTAuth Services supported by MNOs



○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

OTAuth Services supported by MNOs



Help

195****4021

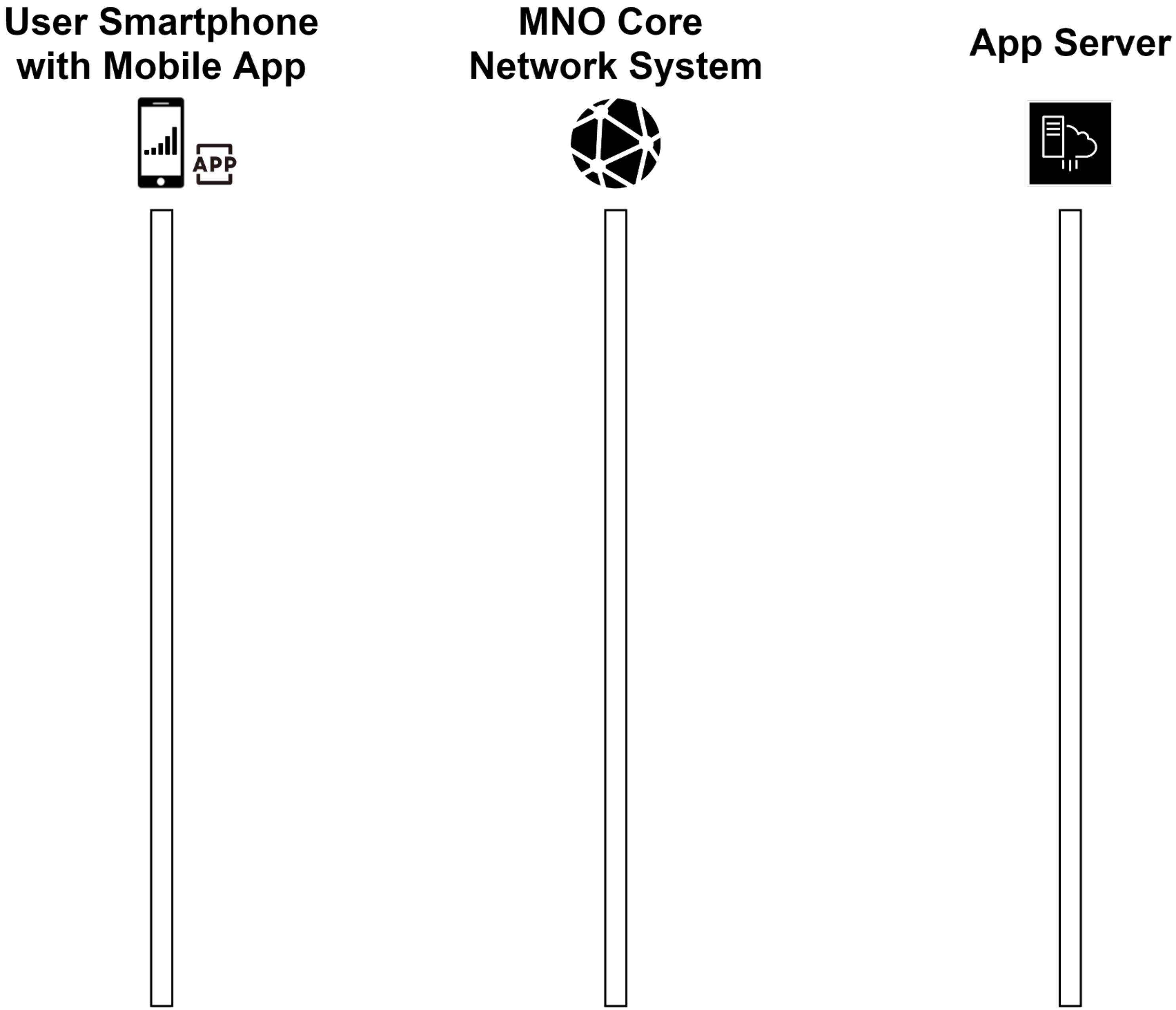
One-click login

WeChat Login

More Options

○ I authorize Kwai to use this phone number and have read and agreed to the following policies: Terms of Service, Privacy Protection Policy, Child protection agreement, Data protection policy for users under 18 and China Mobile Certification Terms of Service

Key design of the OTAuth Scheme

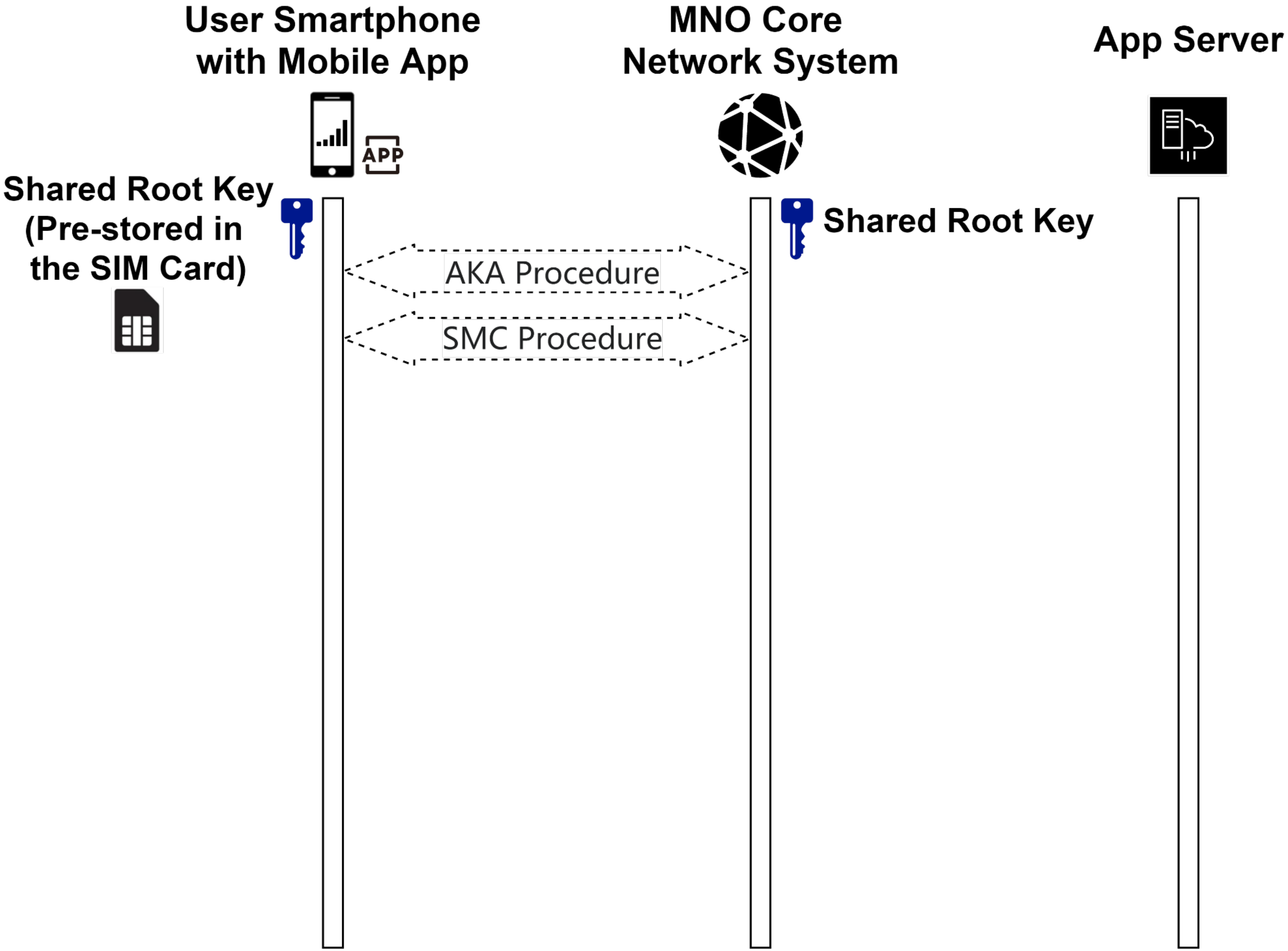


User Smartphone with Mobile App

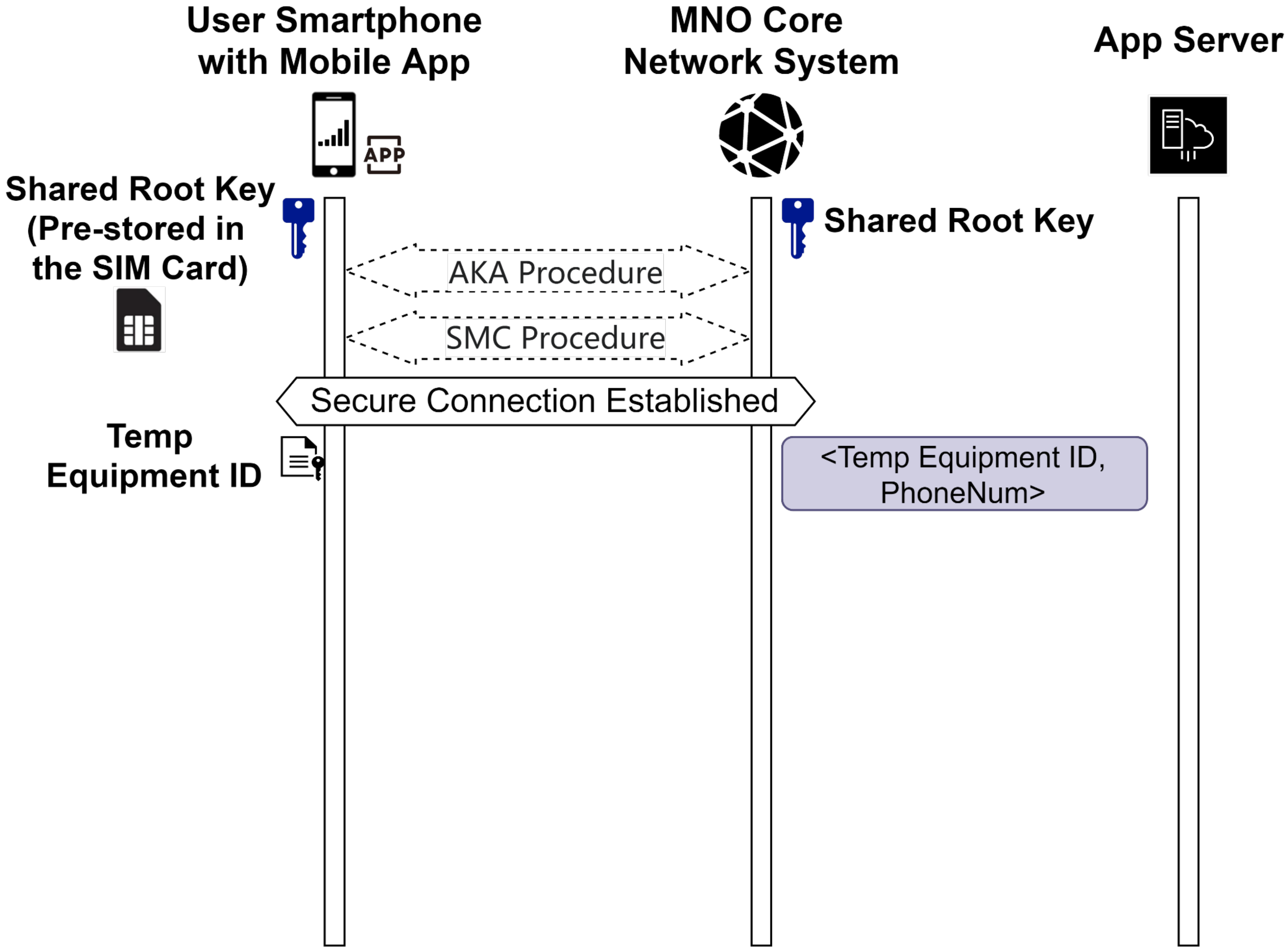
MNO Core Network System

App Server

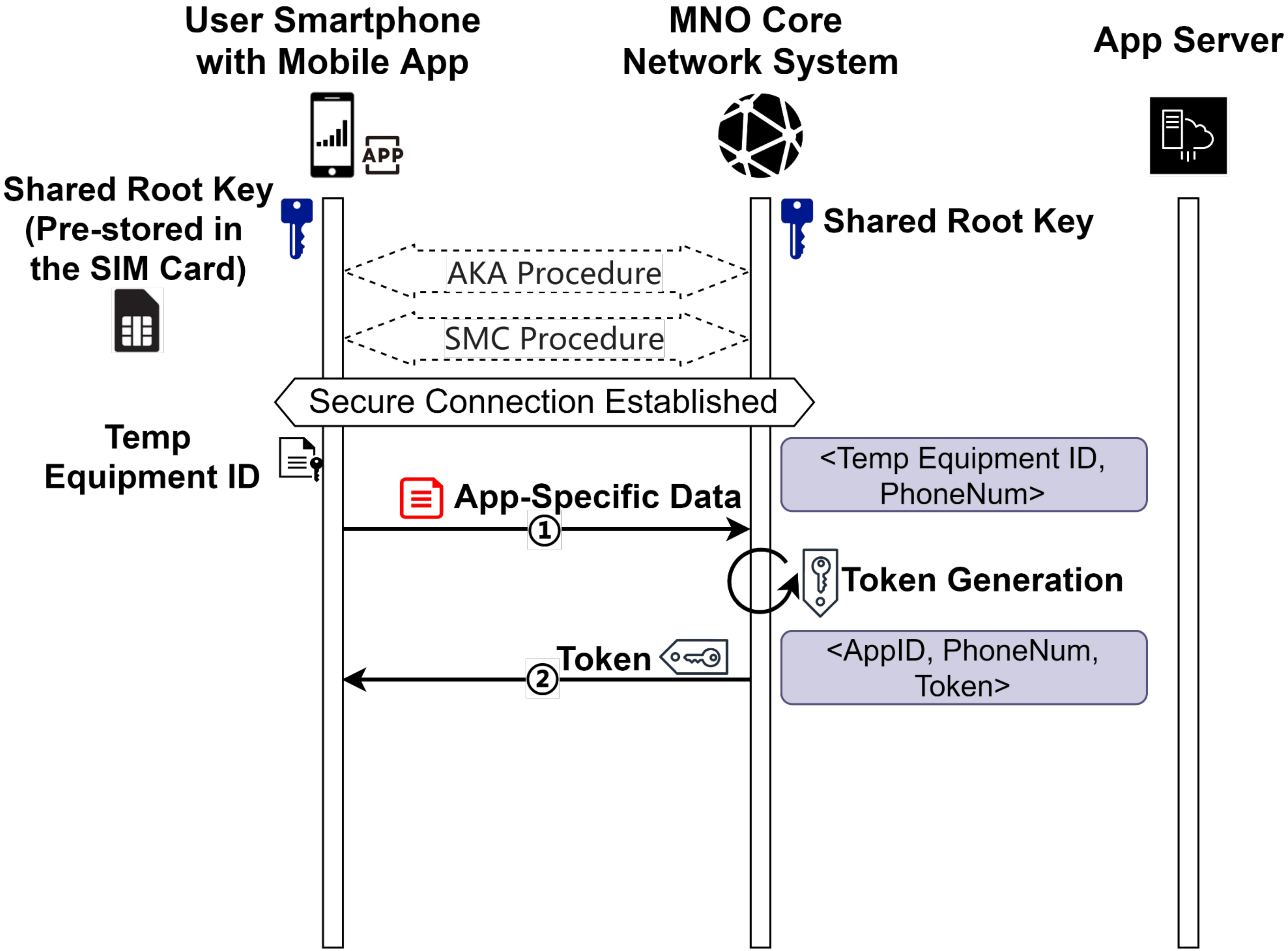
Key design of the OTAuth Scheme



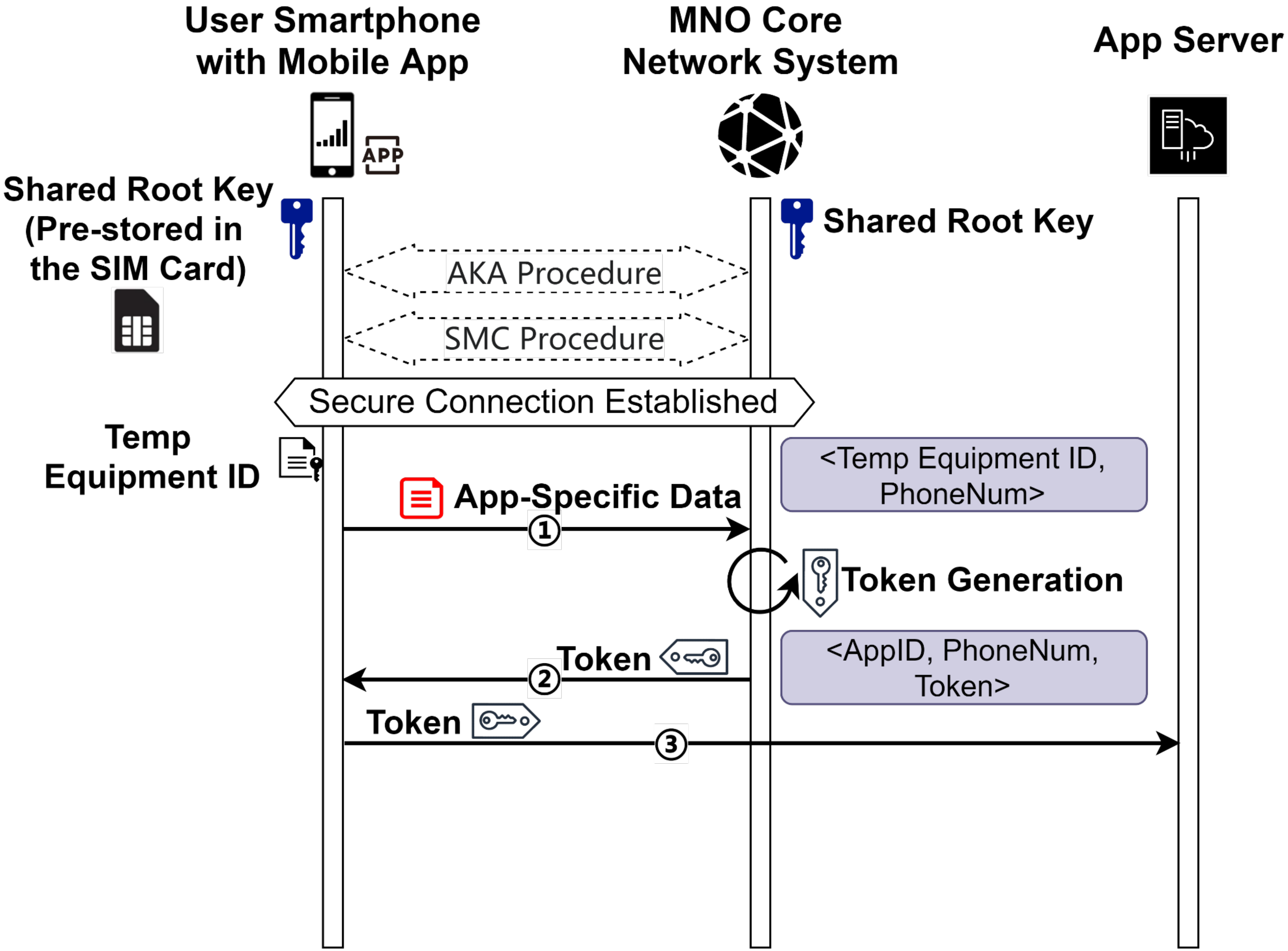
Key design of the OTAuth Scheme


User Smartphone with Mobile App
MNO Core Network System
App Server
APP
Shared Root Key (Pre-stored in the SIM Card)
Shared Root Key
AKA Procedure
SMC Procedure
Secure Connection Established
Temp Equipment ID
<Temp Equipment ID, PhoneNum>

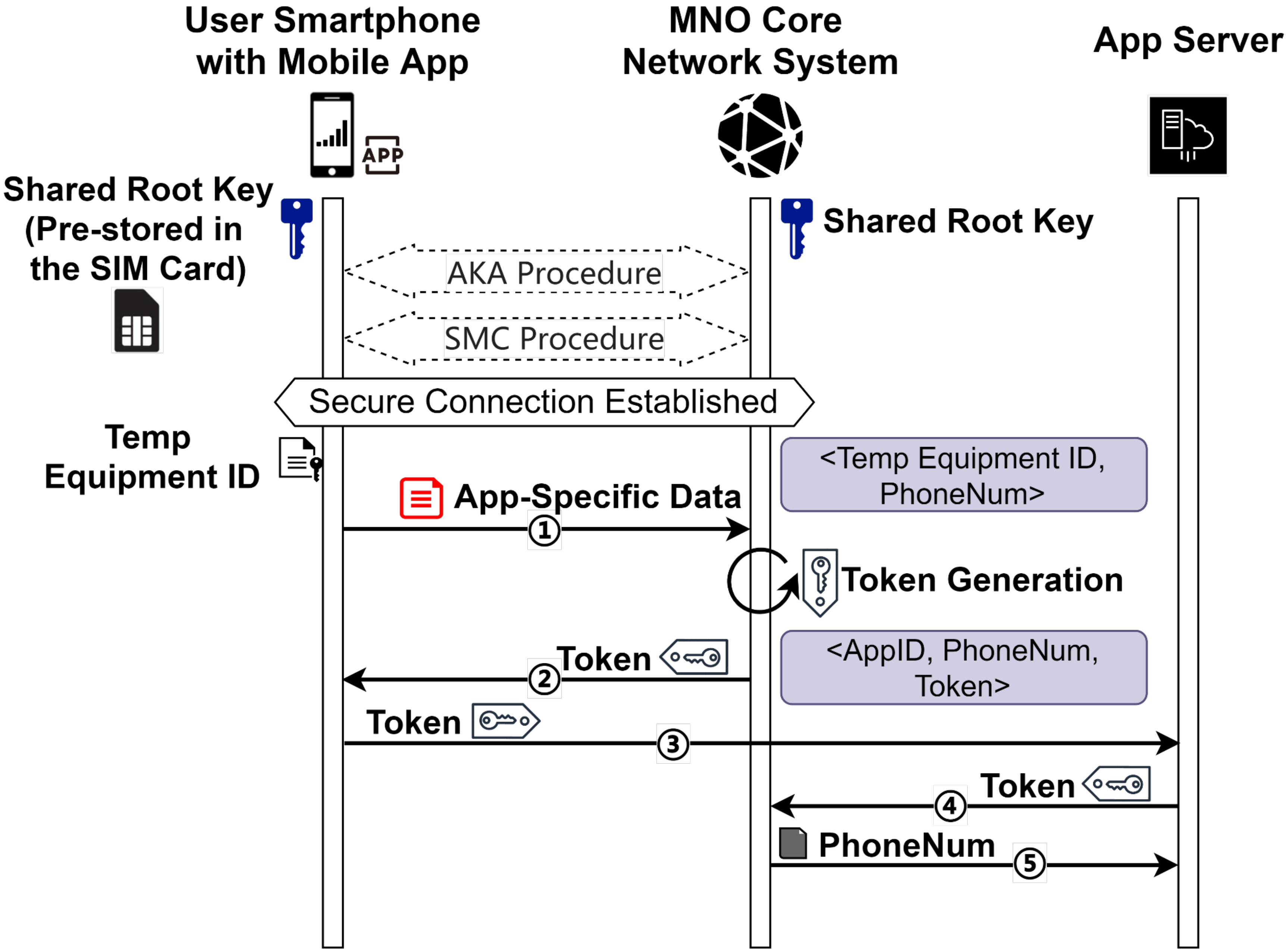
Key design of the OTAuth Scheme



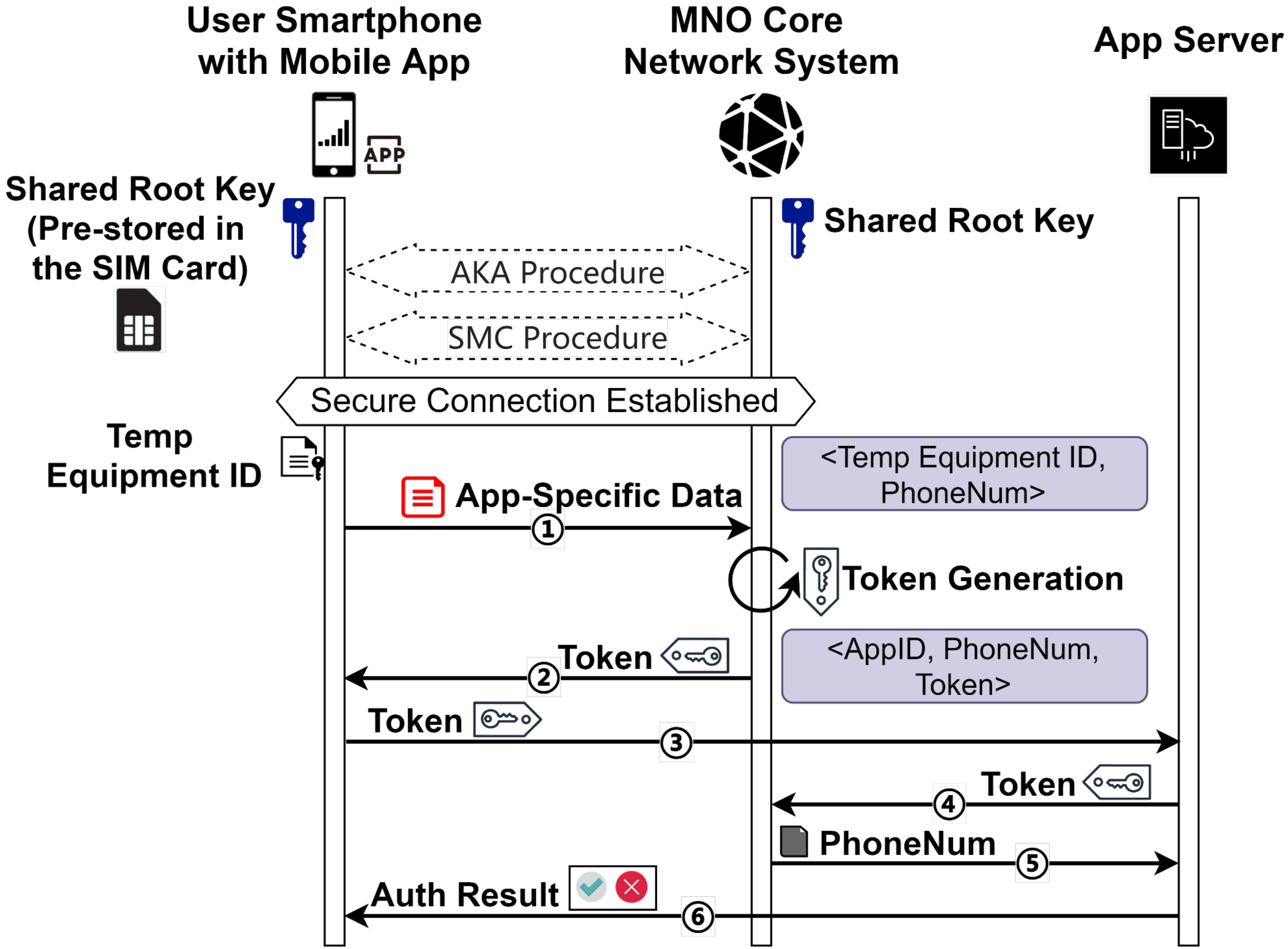
Key design of the OTAuth Scheme



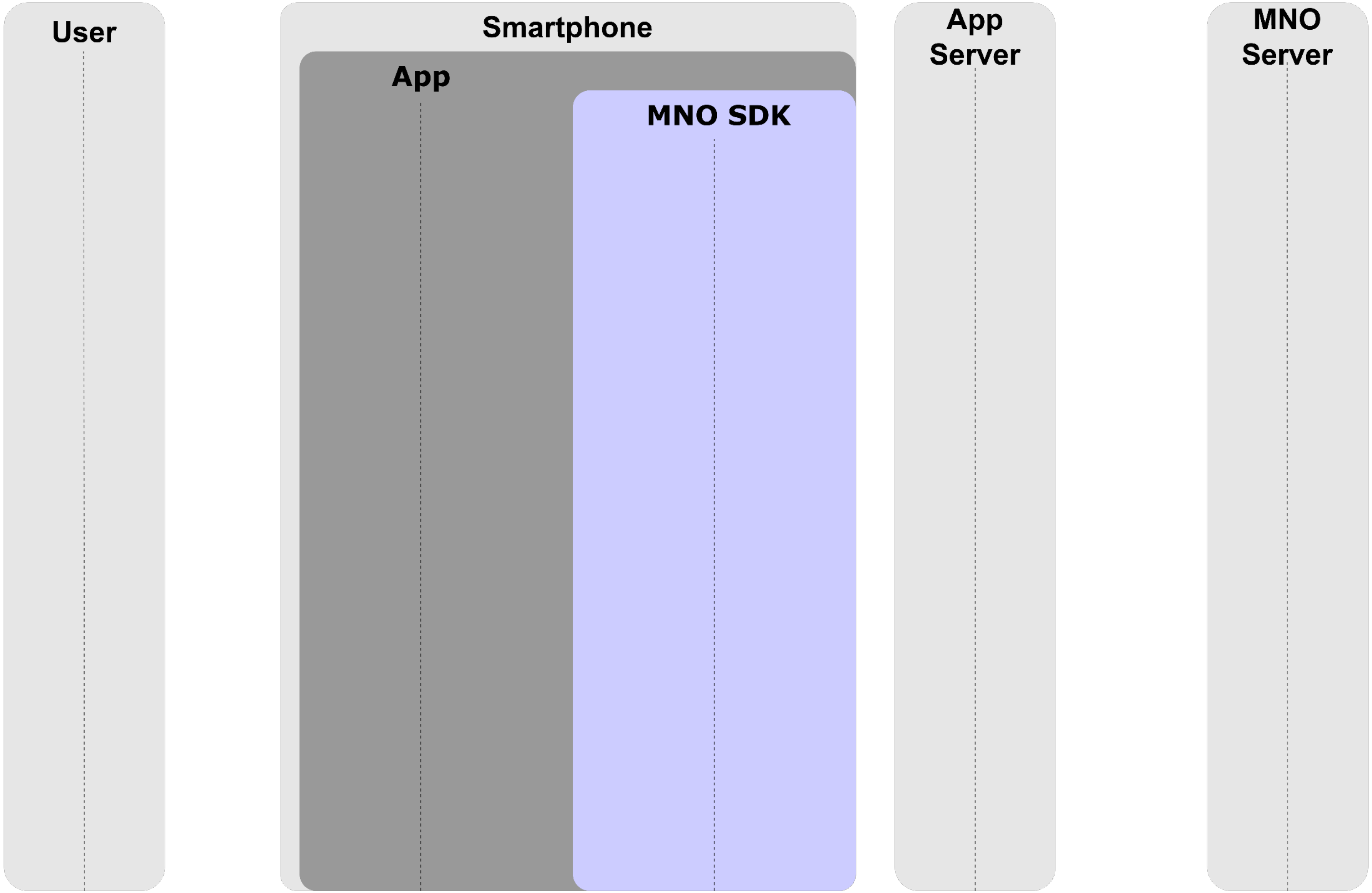
Key design of the OTAuth Scheme



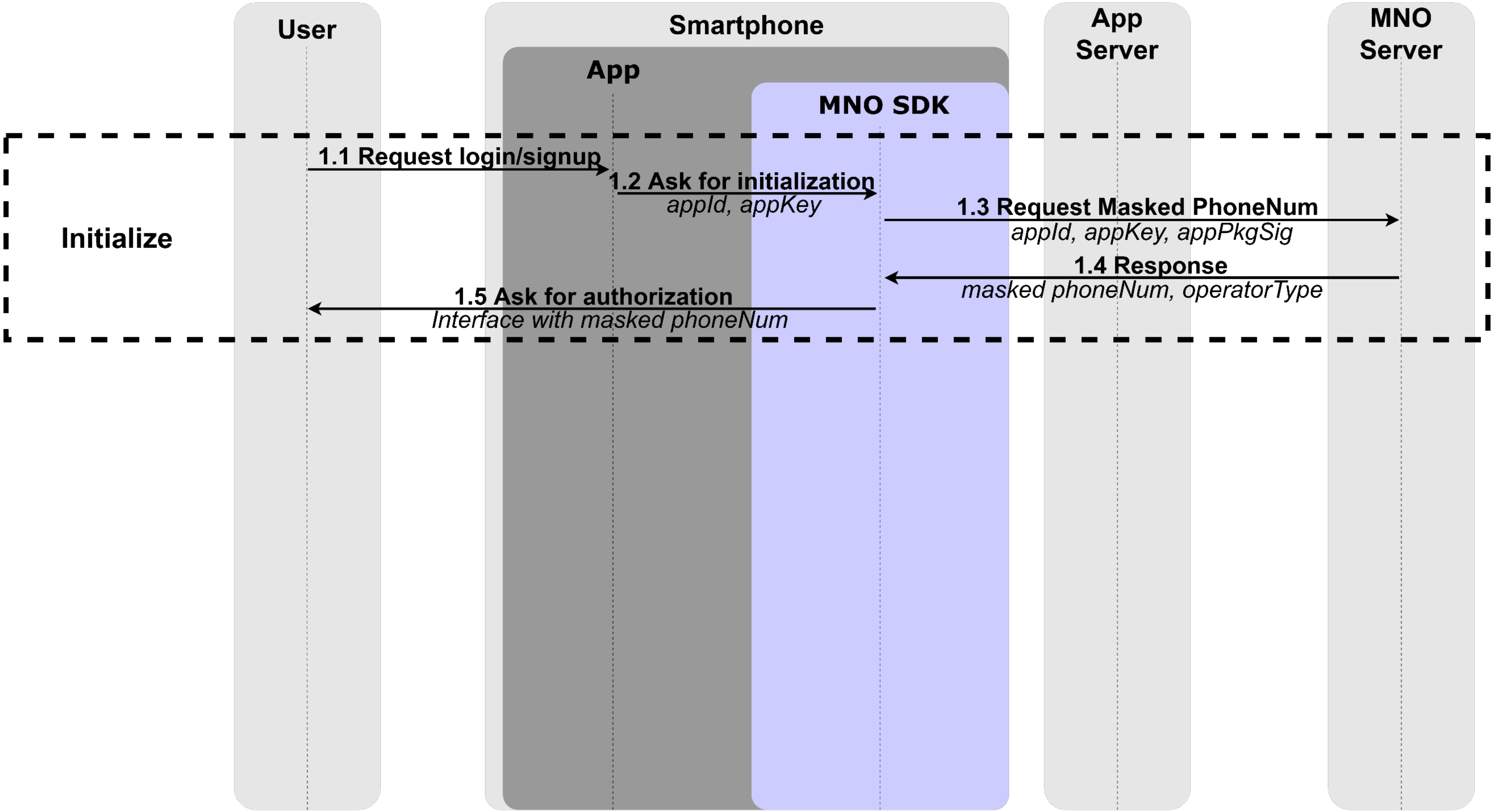
Key design of the OTAuth Scheme



OTAuth Scheme Details



OTAuth Scheme Details



User

Smartphone

App

MNO SDK

App Server

MNO Server

Initialize

1.1 Request login/signup

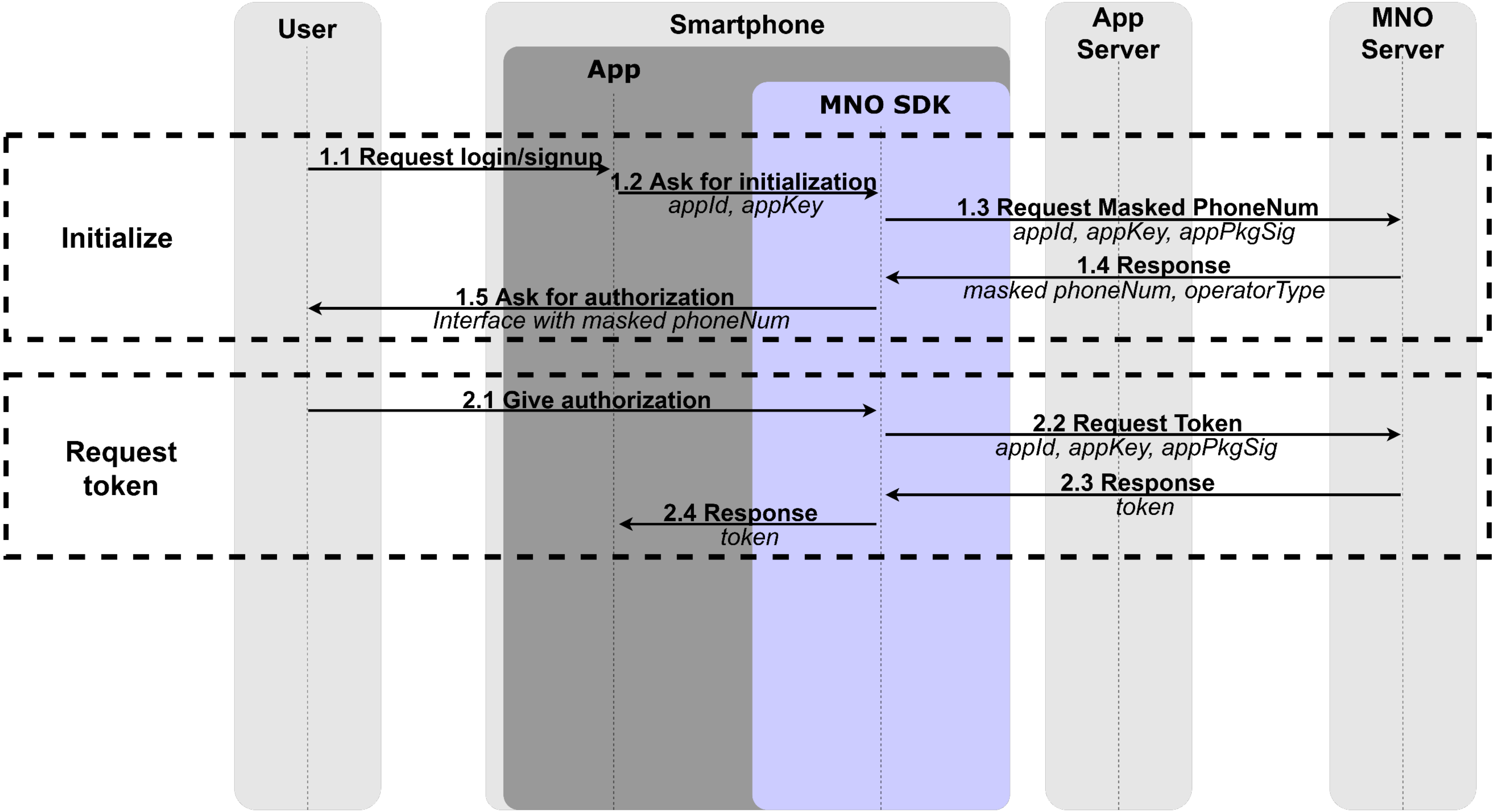
1.2 Ask for initialization
appId, appKey

1.3 Request Masked PhoneNum
appId, appKey, appPkgSig

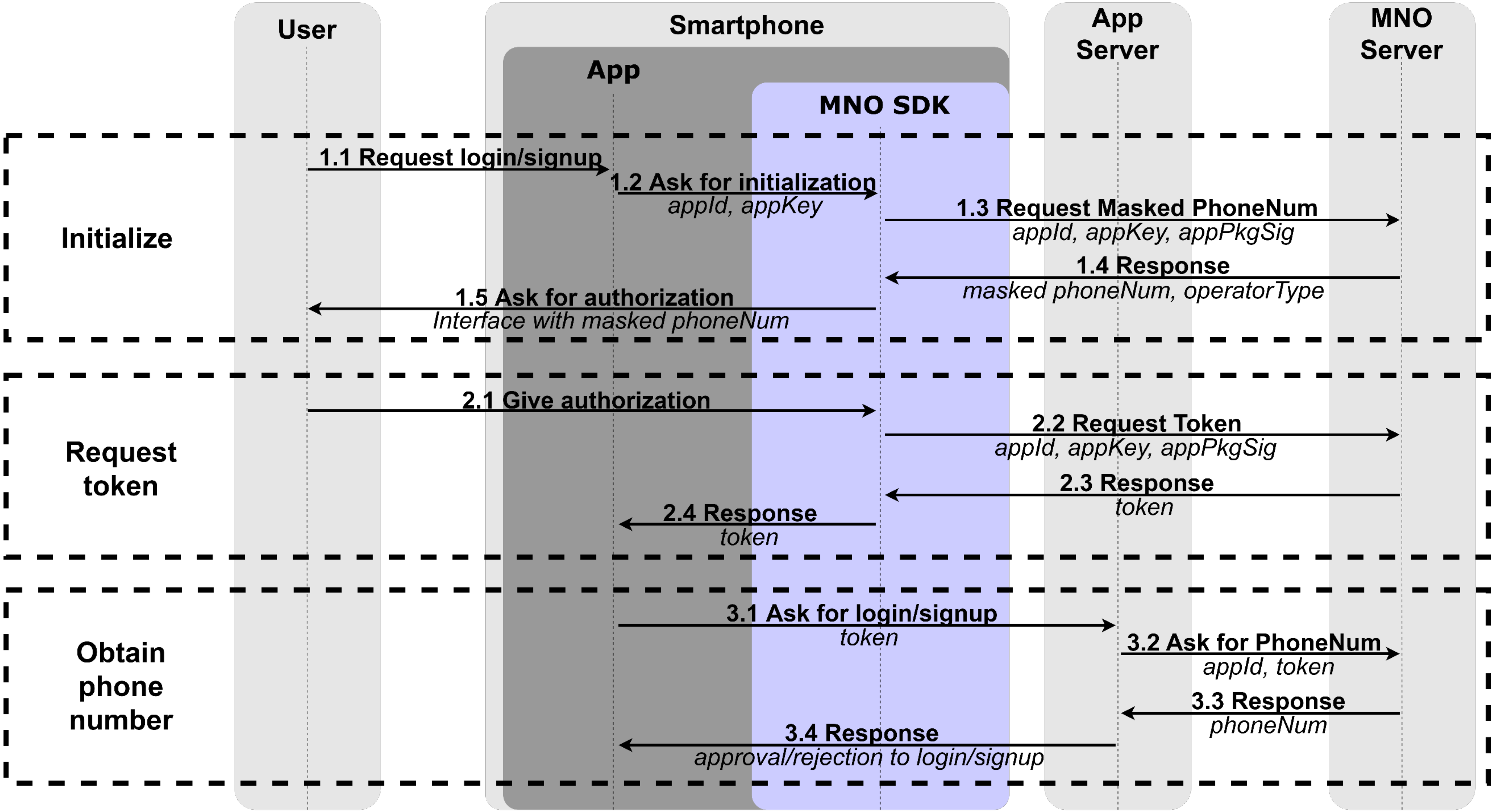
1.4 Response
masked phoneNum, operatorType

1.5 Ask for authorization
Interface with masked phoneNum

OTAuth Scheme Details

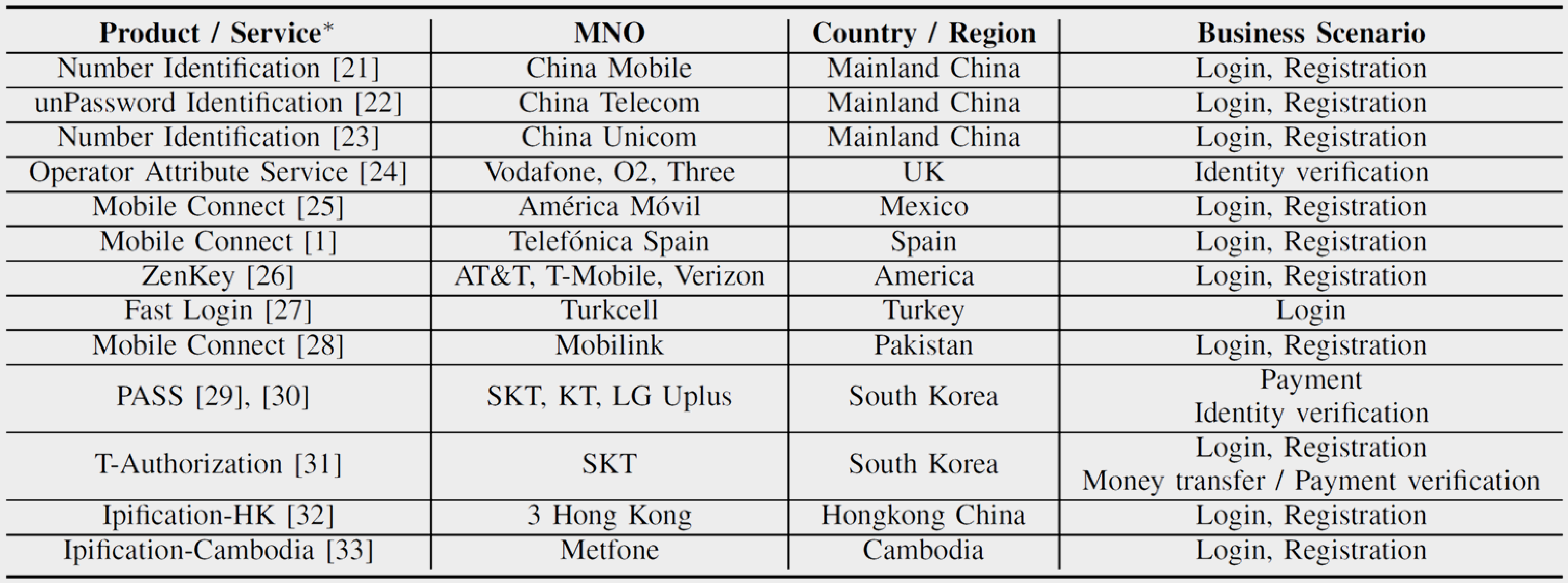


OTAuth Scheme Details



Scope of Our Study

Typical OTAuth services worldwide (ranked by MNO's total number of subscriptions)



Product / Service*	MNO	Country / Region	Business Scenario
Number Identification [21]	China Mobile	Mainland China	Login, Registration
unPassword Identification [22]	China Telecom	Mainland China	Login, Registration
Number Identification [23]	China Unicom	Mainland China	Login, Registration
Operator Attribute Service [24]	Vodafone, O2, Three	UK	Identity verification
Mobile Connect [25]	América Móvil	Mexico	Login, Registration
Mobile Connect [1]	Telefónica Spain	Spain	Login, Registration
ZenKey [26]	AT&T, T-Mobile, Verizon	America	Login, Registration
Fast Login [27]	Turkcell	Turkey	Login
Mobile Connect [28]	Mobilink	Pakistan	Login, Registration
PASS [29], [30]	SKT, KT, LG Uplus	South Korea	Payment Identity verification
T-Authorization [31]	SKT	South Korea	Login, Registration Money transfer / Payment verification
Ipification-HK [32]	3 Hong Kong	Hongkong China	Login, Registration
Ipification-Cambodia [33]	Metfone	Cambodia	Login, Registration

* This table demonstrates the prevalence of mobile OTAuth services worldwide but does **not** imply all of them are vulnerable.

In our research, we only confirmed the first three services in mainland China are vulnerable for the **SIMulation** attack.

Attack Model

Attack Model

- **Assumption on the attacker:**

  Under either of the following scenarios:

Attack Model

- **Assumption on the attacker:**

  Under either of the following scenarios:

  - **Scenario 1: The attacker can install an innocent looking malicious app to the victim's device**
    - Only needs the INTERNET permission

Attack Model

- **Assumption on the attacker:**

  Under either of the following scenarios:

  - **Scenario 1: The attacker can install an innocent looking malicious app to the victim's device**
    - Only needs the INTERNET permission
  - **Scenario 2: The attacker is within the same network as the victim's device**
    - Typically happens when the attacker connects to the hotspot shared by the victim's device

Attack Model

- **Assumption on the attacker:**

  Under either of the following scenarios:

  - **Scenario 1: The attacker can install an innocent looking malicious app to the victim's device**
    - Only needs the INTERNET permission
  - **Scenario 2: The attacker is within the same network as the victim's device**
    - Typically happens when the attacker connects to the hotspot shared by the victim's device

- **Assumption on the victim:**

Attack Model

- **Assumption on the attacker:**

  Under either of the following scenarios:

  - **Scenario 1: The attacker can install an innocent looking malicious app to the victim's device**
    - Only needs the INTERNET permission
  - **Scenario 2: The attacker is within the same network as the victim's device**
    - Typically happens when the attacker connects to the hotspot shared by the victim's device

- **Assumption on the victim:**
  - **There is a SIM card on the victim's smartphone**
  - **The Mobile Data switch has been turned on**

Attack Model

- **Assumption on the attacker:**

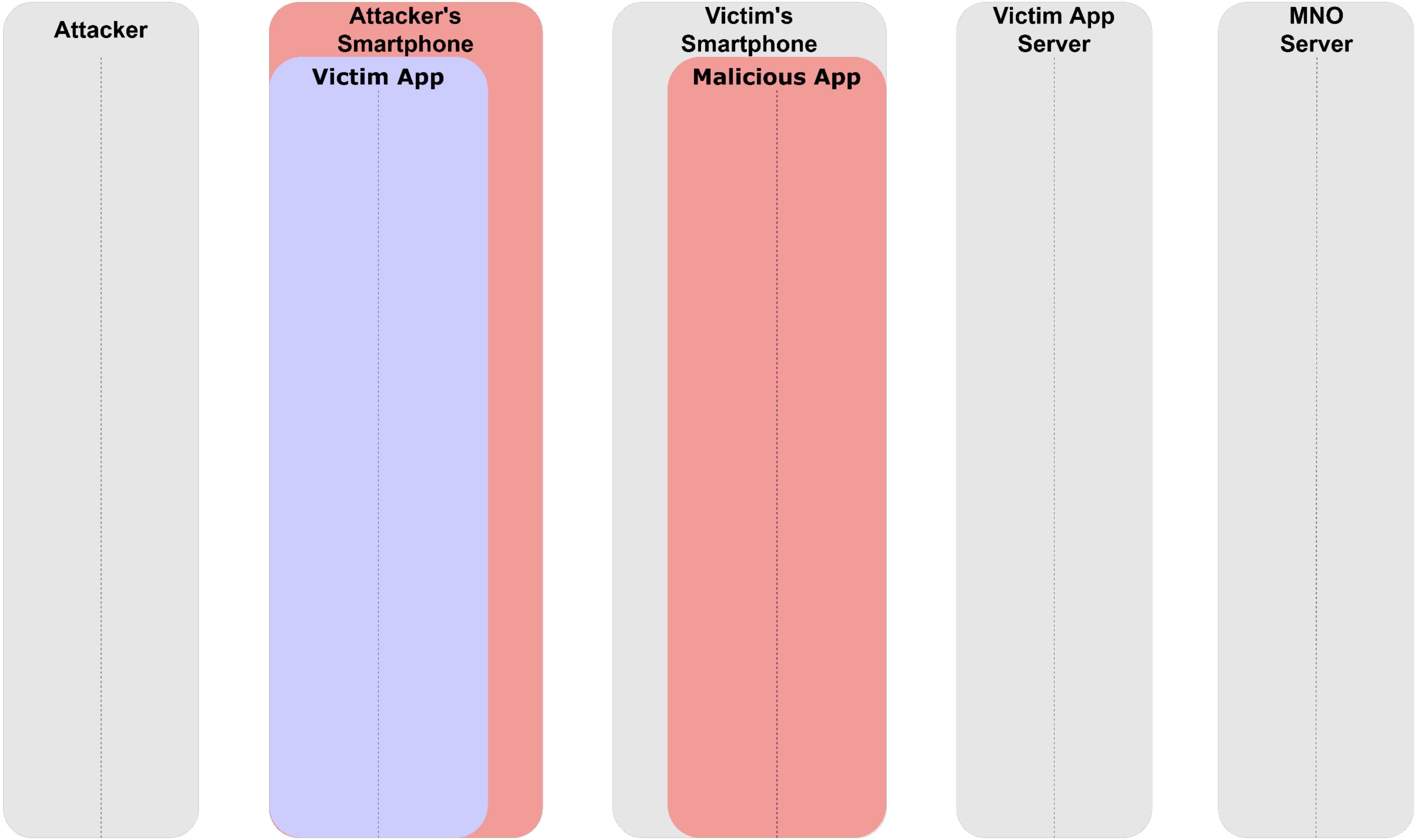
  Under either of the following scenarios:

  - ■ **Scenario 1: The attacker can install an innocent looking malicious app to the victim's device**
    - ◆ Only needs the INTERNET permission
  - ■ **Scenario 2: The attacker is within the same network as the victim's device**
    - ◆ Typically happens when the attacker connects to the hotspot shared by the victim's device

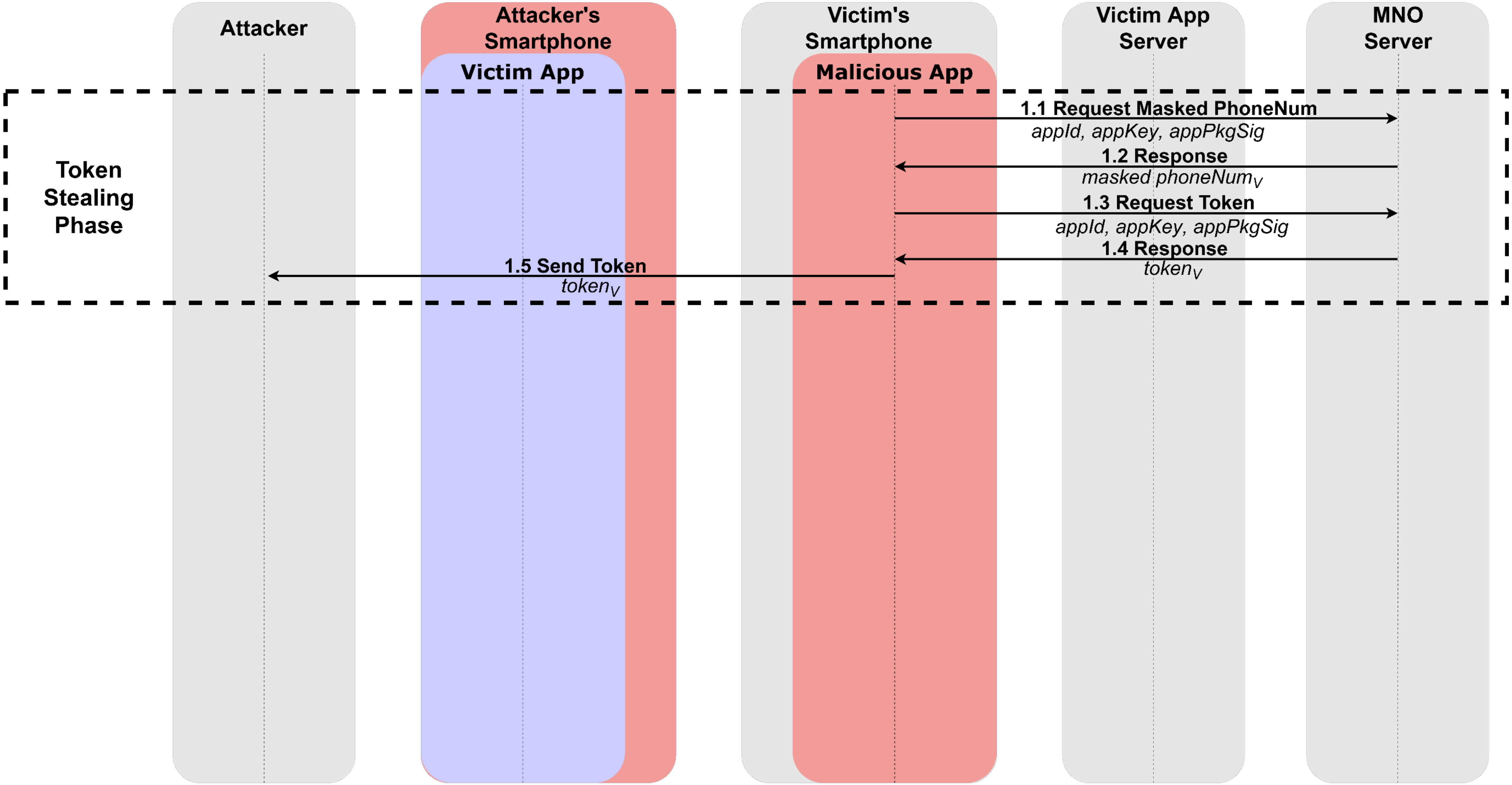
- **Assumption on the victim:**
  - ■ **There is a SIM card on the victim's smartphone**
  - ■ **The Mobile Data switch has been turned on**

  ※ **The attack can succeed regardless of whether the WLAN switch has been turned on**

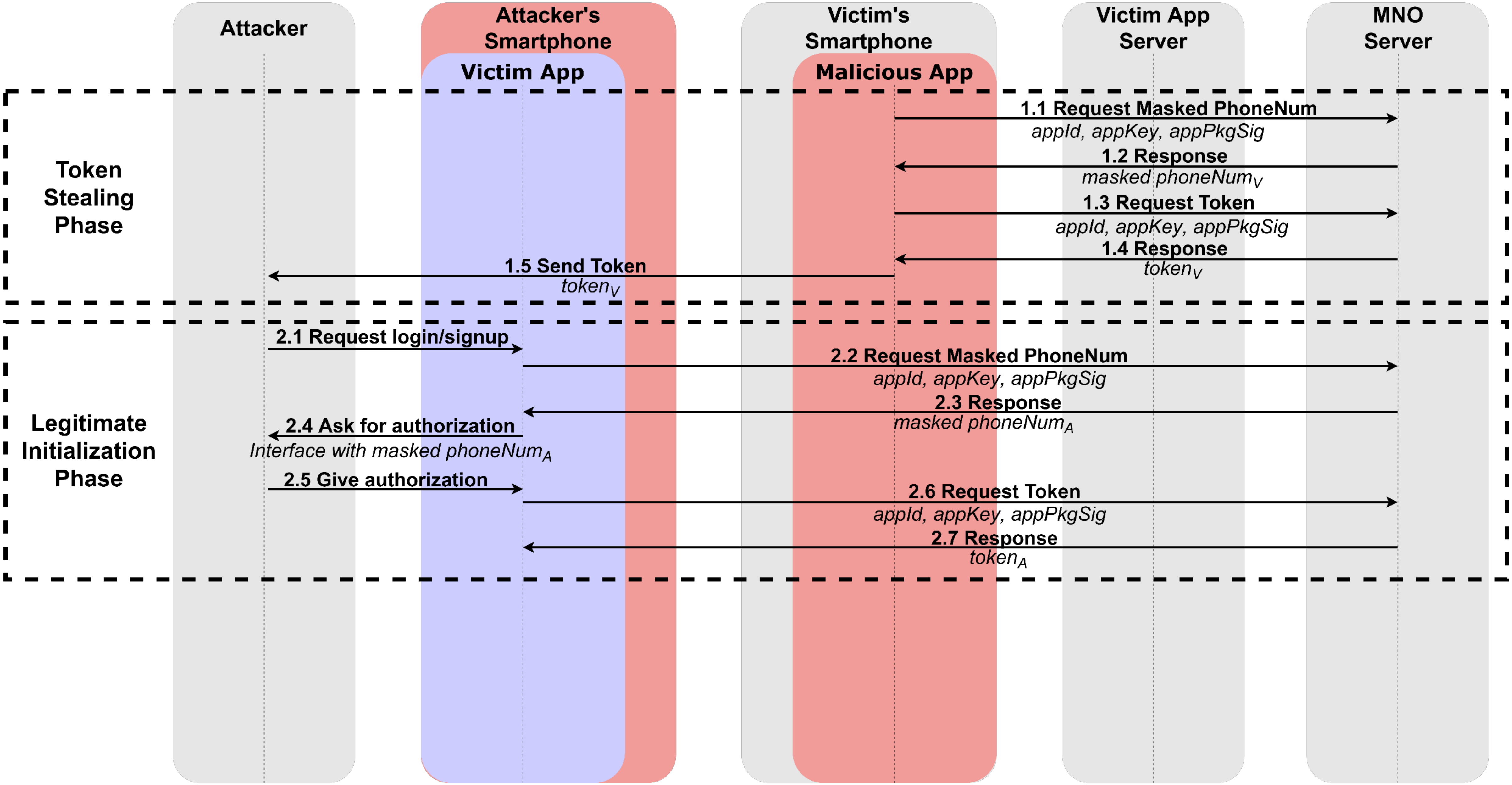
Attack Details



Attack Details



Attack Details



Attacker

Attacker's Smartphone

Victim App

Victim's Smartphone

Malicious App

Victim App Server

MNO Server

Token Stealing Phase

1.1 Request Masked PhoneNum

appId, appKey, appPkgSig

1.2 Response

masked phoneNum$_V$

1.3 Request Token

appId, appKey, appPkgSig

1.4 Response

token$_V$

1.5 Send Token

token$_V$

Legitimate Initialization Phase

2.1 Request login/signup

2.2 Request Masked PhoneNum

appId, appKey, appPkgSig

2.3 Response

masked phoneNum$_A$

2.4 Ask for authorization

Interface with masked phoneNum$_A$

2.5 Give authorization

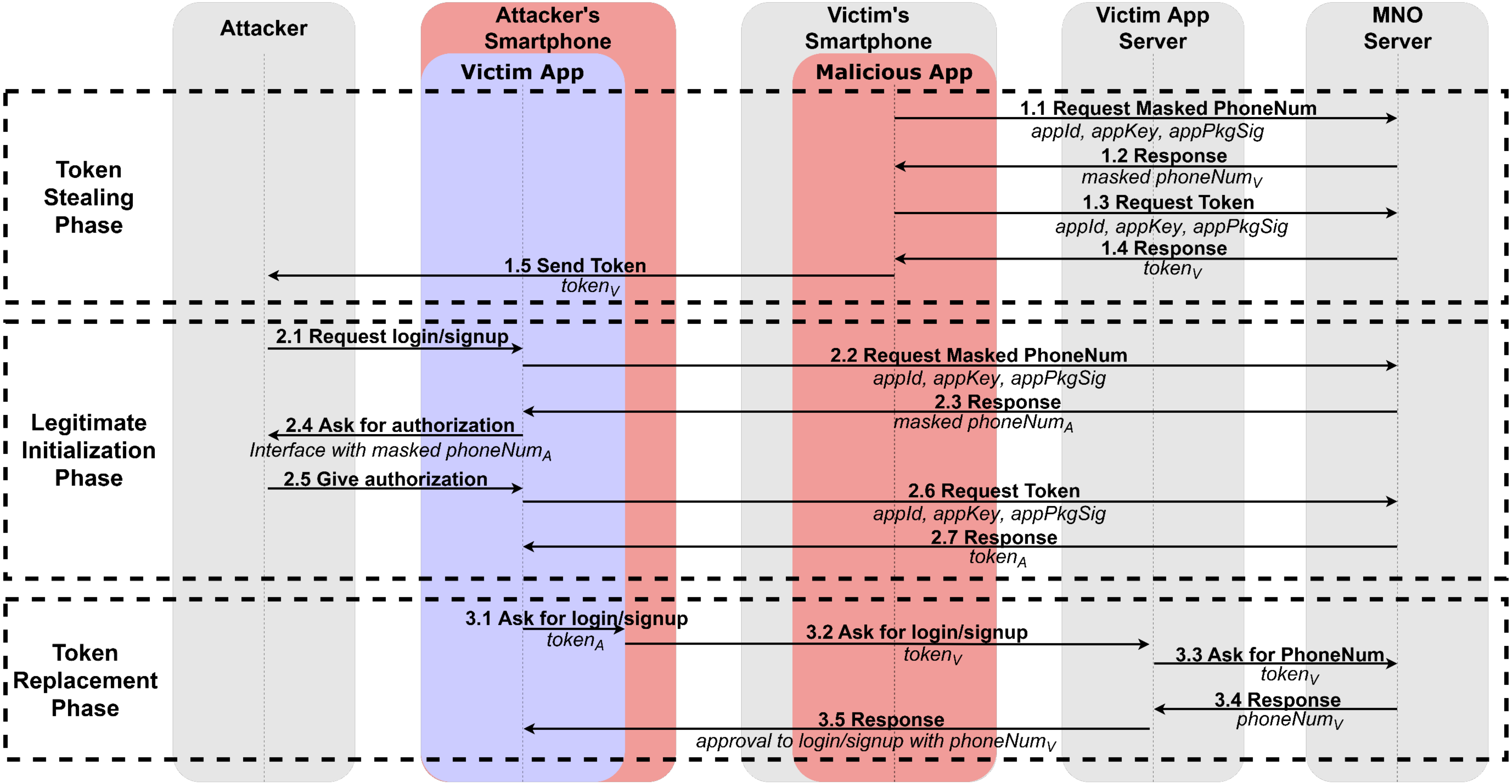
2.6 Request Token

appId, appKey, appPkgSig

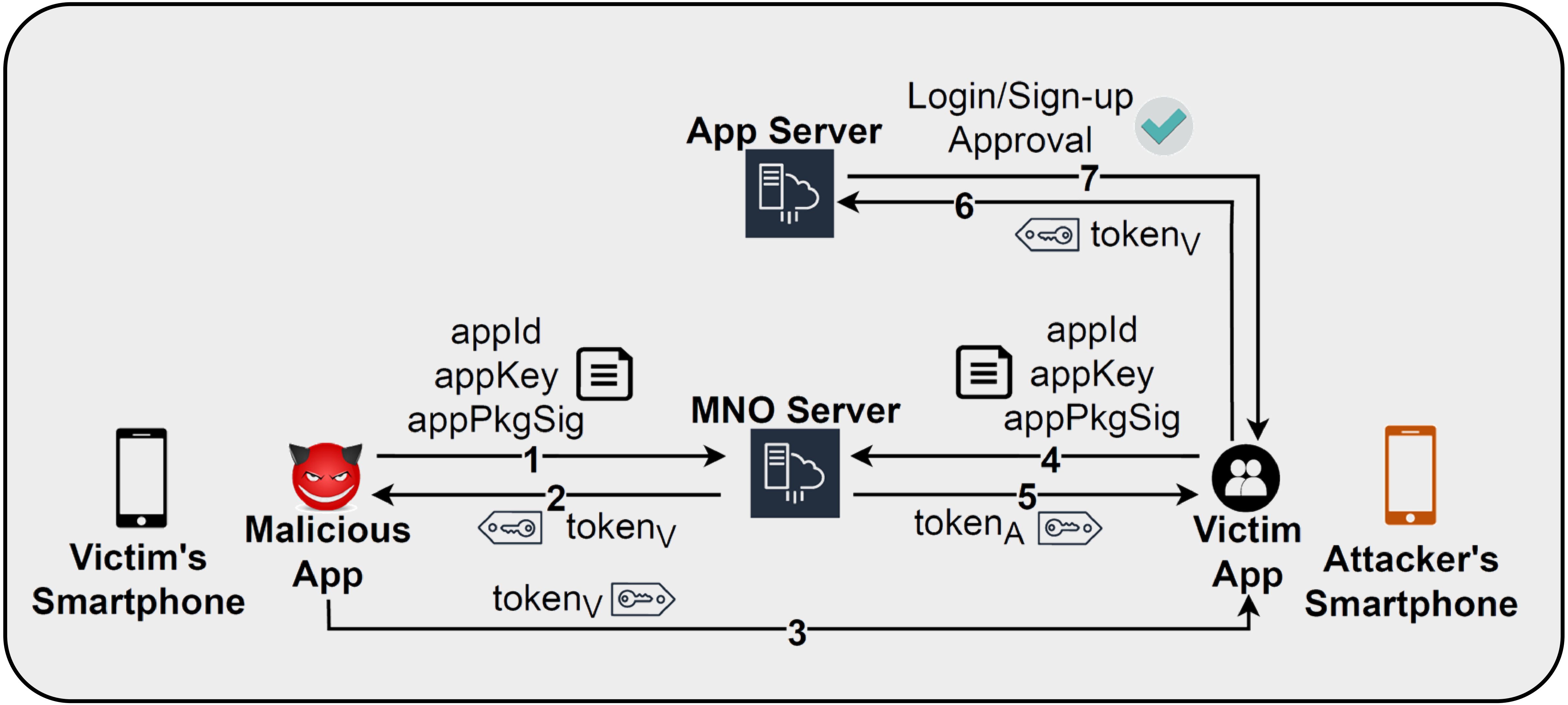
2.7 Response

token$_A$

Attack Details

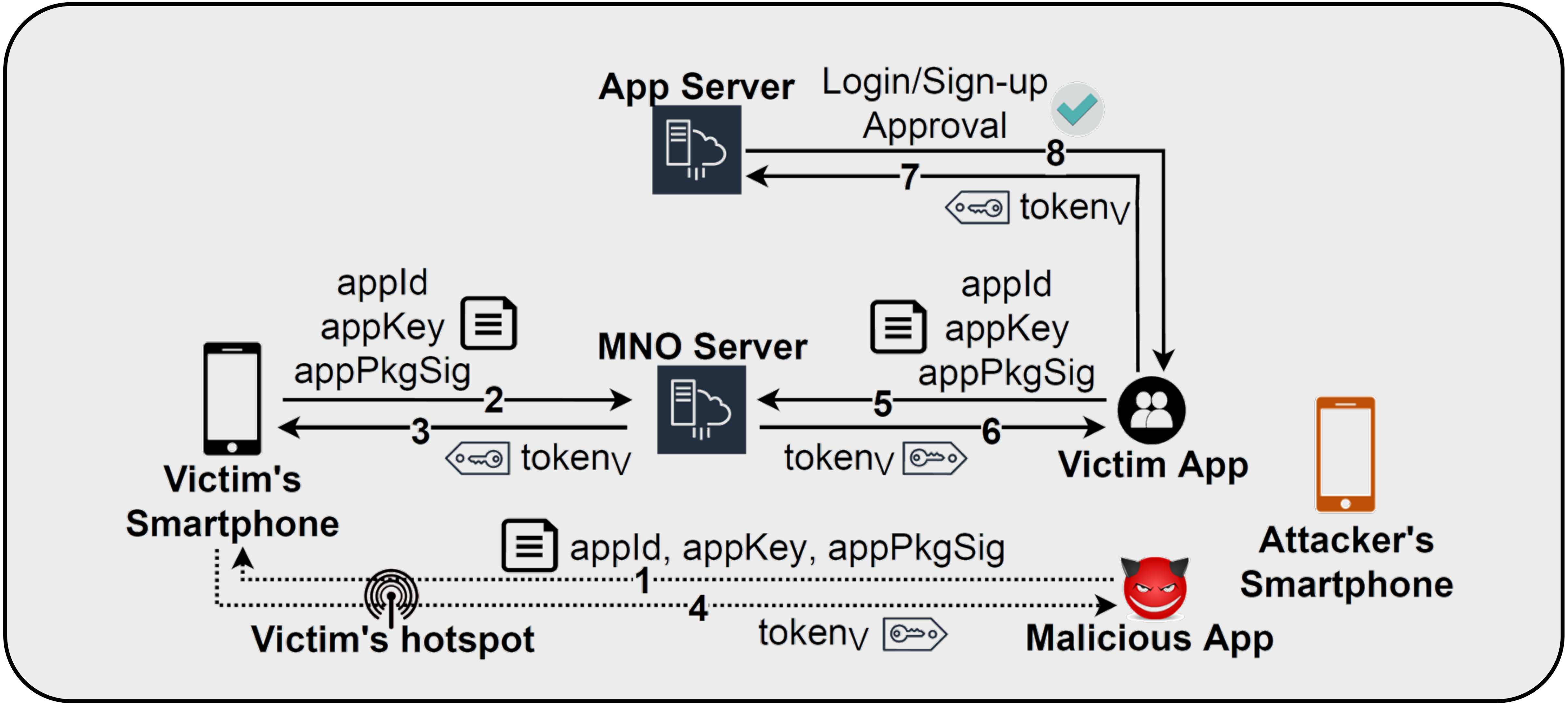


Attack Implementation



Scenario 1: Attack via a malicious app

Attack Implementation



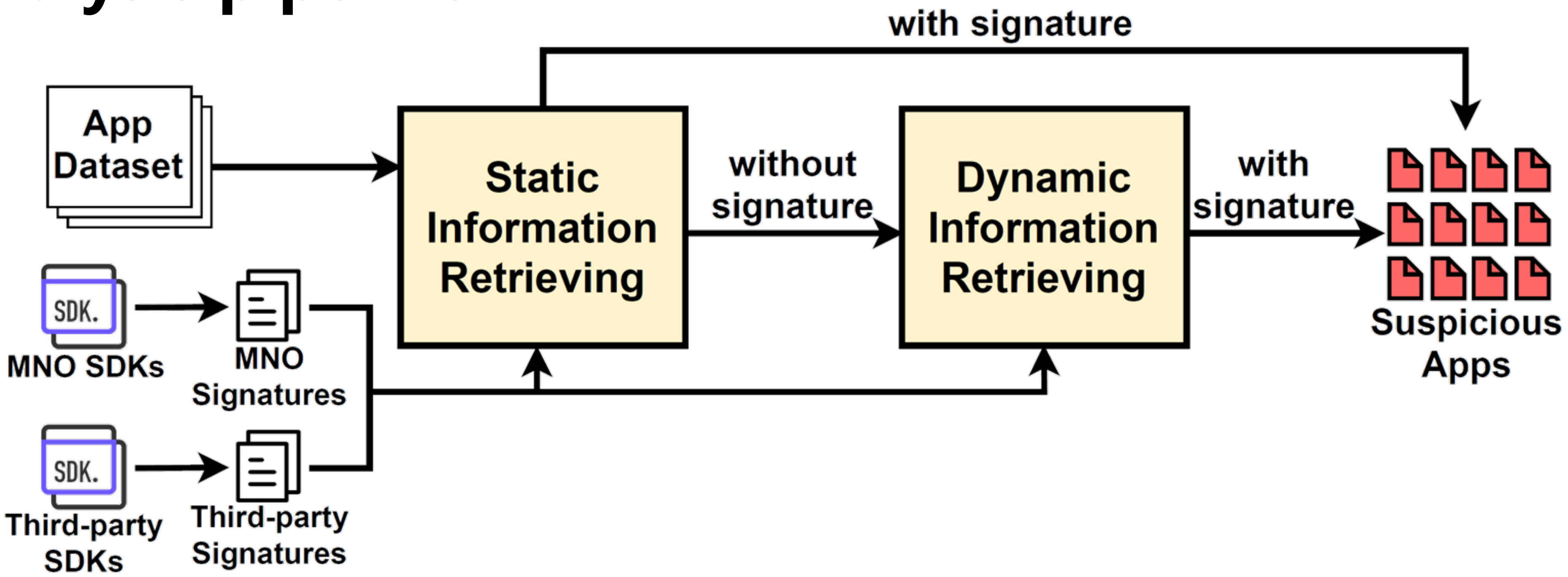
Scenario 2: Attack by connecting to victim's hotspot

Large-scale Measurement

- **Dataset**
  - 1,025 top Android apps from Huawei App Store and 894 top iOS apps from Apple App Store
    Each app holds more than 100 million downloads
  - 3 MNO SDKs and 19 third-party SDKs

Large-scale Measurement

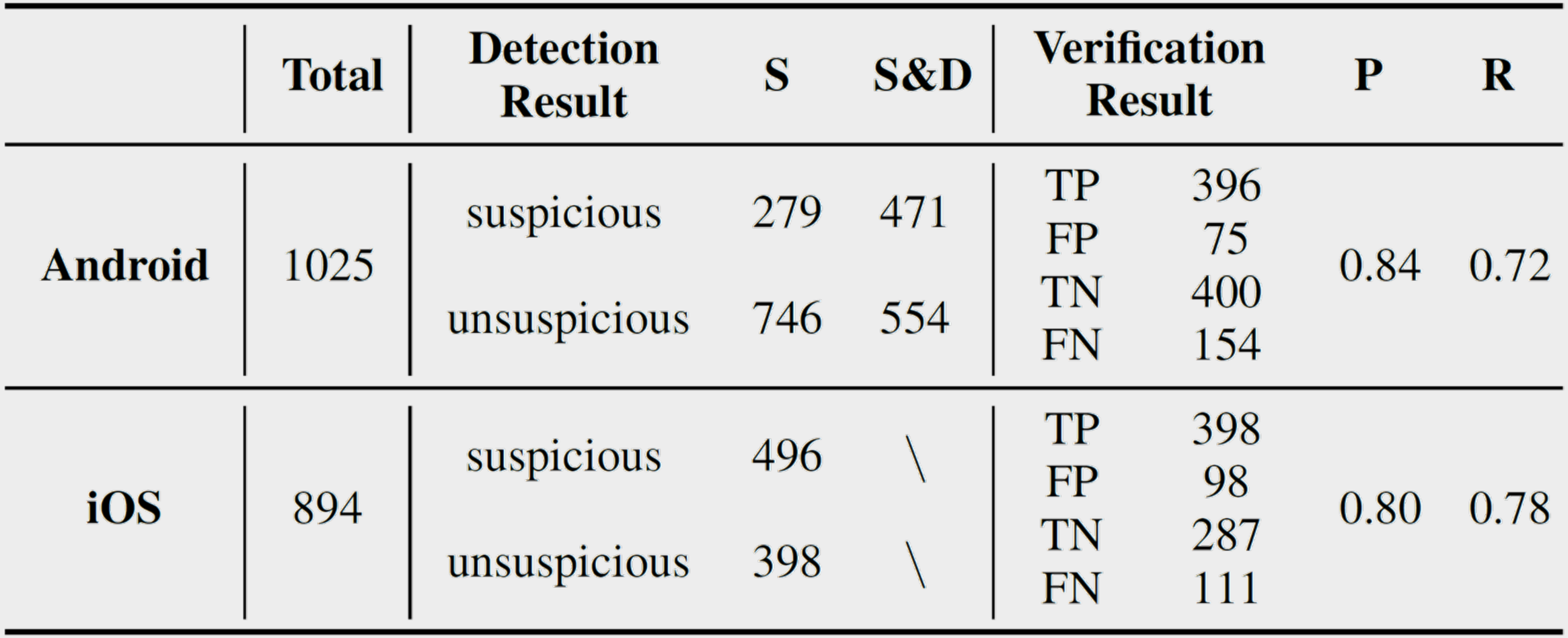
- **Dataset**
  - 1,025 top Android apps from Huawei App Store and 894 top iOS apps from Apple App Store
    Each app holds more than 100 million downloads
  - 3 MNO SDKs and 19 third-party SDKs
- **Analysis pipeline**



Results and Findings

- **Affected Apps**

App measurement results



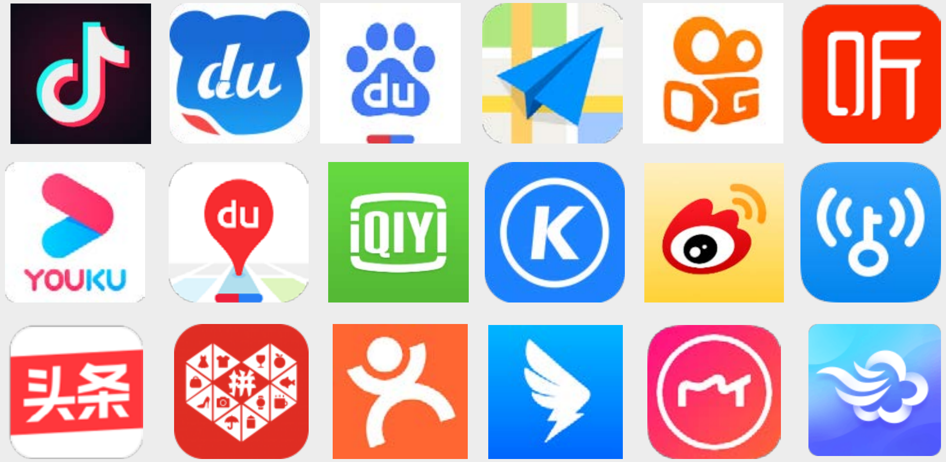
	Total	Detection Result	S	S&D	Verification Result		P	R
Android	1025	suspicious	279	471	TP FP	396 75	0.84	0.72
		unsuspicious	746	554	TN FN	400 154		
iOS	894	suspicious	496	\	TP FP	398 98	0.80	0.78
		unsuspicious	398	\	TN FN	287 111		

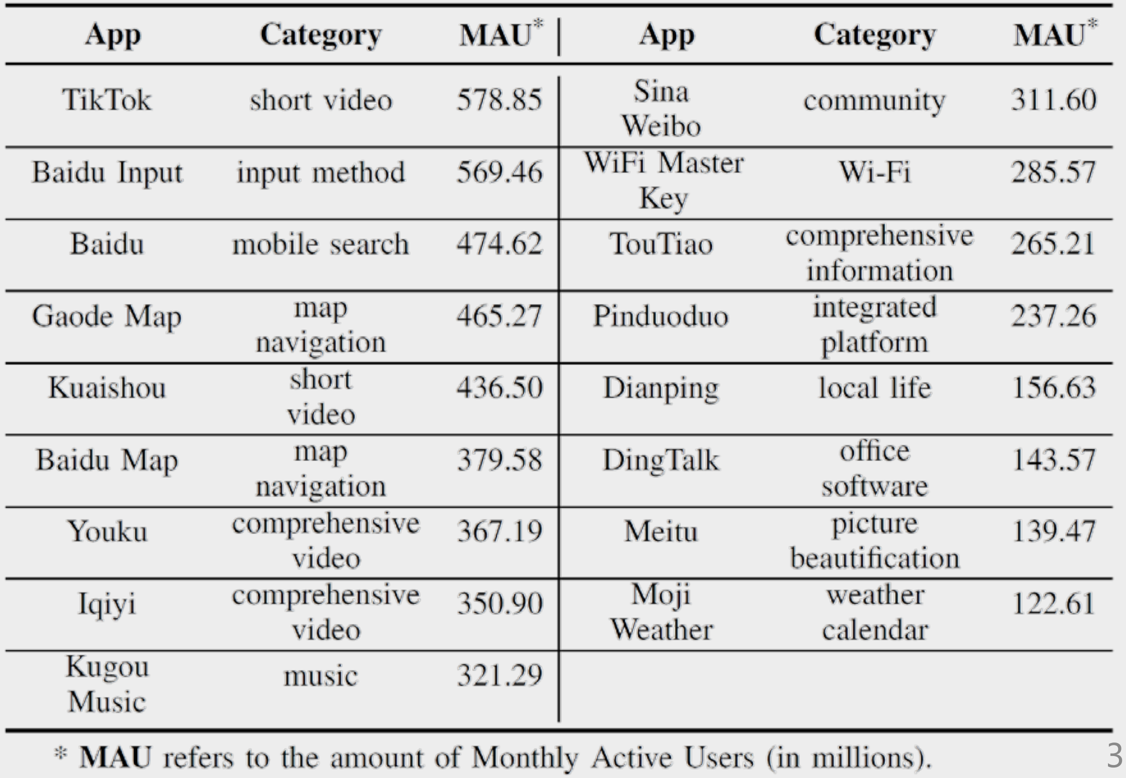
□ We manually confirmed that **396 Android apps (38.6%)** and **398 iOS apps (44.5%)** in our dataset are affected by the attack

Results and Findings

- **17** affected apps have over **100 million** Monthly Active Users
- **87** affected apps have over **10 million** Monthly Active Users

Affected top apps





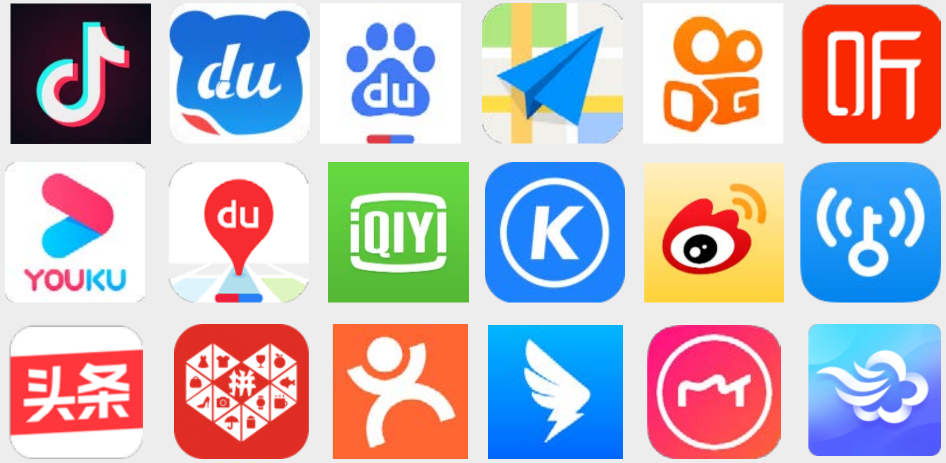
App	Category	MAU*	App	Category	MAU*
TikTok	short video	578.85	Sina Weibo	community	311.60
Baidu Input	input method	569.46	WiFi Master Key	Wi-Fi	285.57
Baidu	mobile search	474.62	TouTiao	comprehensive information	265.21
Gaode Map	map navigation	465.27	Pinduoduo	integrated platform	237.26
Kuaishou	short video	436.50	Dianping	local life	156.63
Baidu Map	map navigation	379.58	DingTalk	office software	143.57
Youku	comprehensive video	367.19	Meitu	picture beautification	139.47
Iqiyi	comprehensive video	350.90	Moji Weather	weather calendar	122.61
Kugou Music	music	321.29			

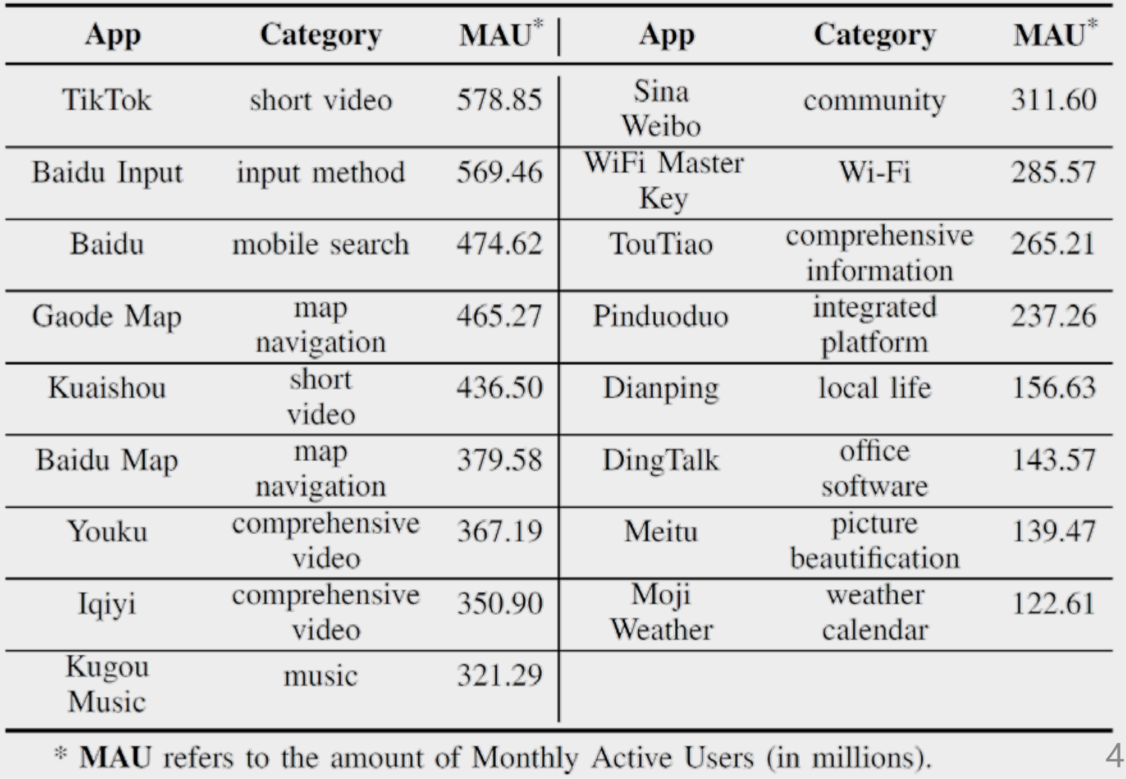
* MAU refers to the amount of Monthly Active Users (in millions).

Results and Findings

- **17** affected apps have over **100 million** Monthly Active Users
- **87** affected apps have over **10 million** Monthly Active Users
- Users of **three major MNOs** in mainland China has surpassed **1 billion** by June 2021
- The OTAuth service of **China Mobile** has been called more than **1.69 trillion** times by October 2021

Affected top apps



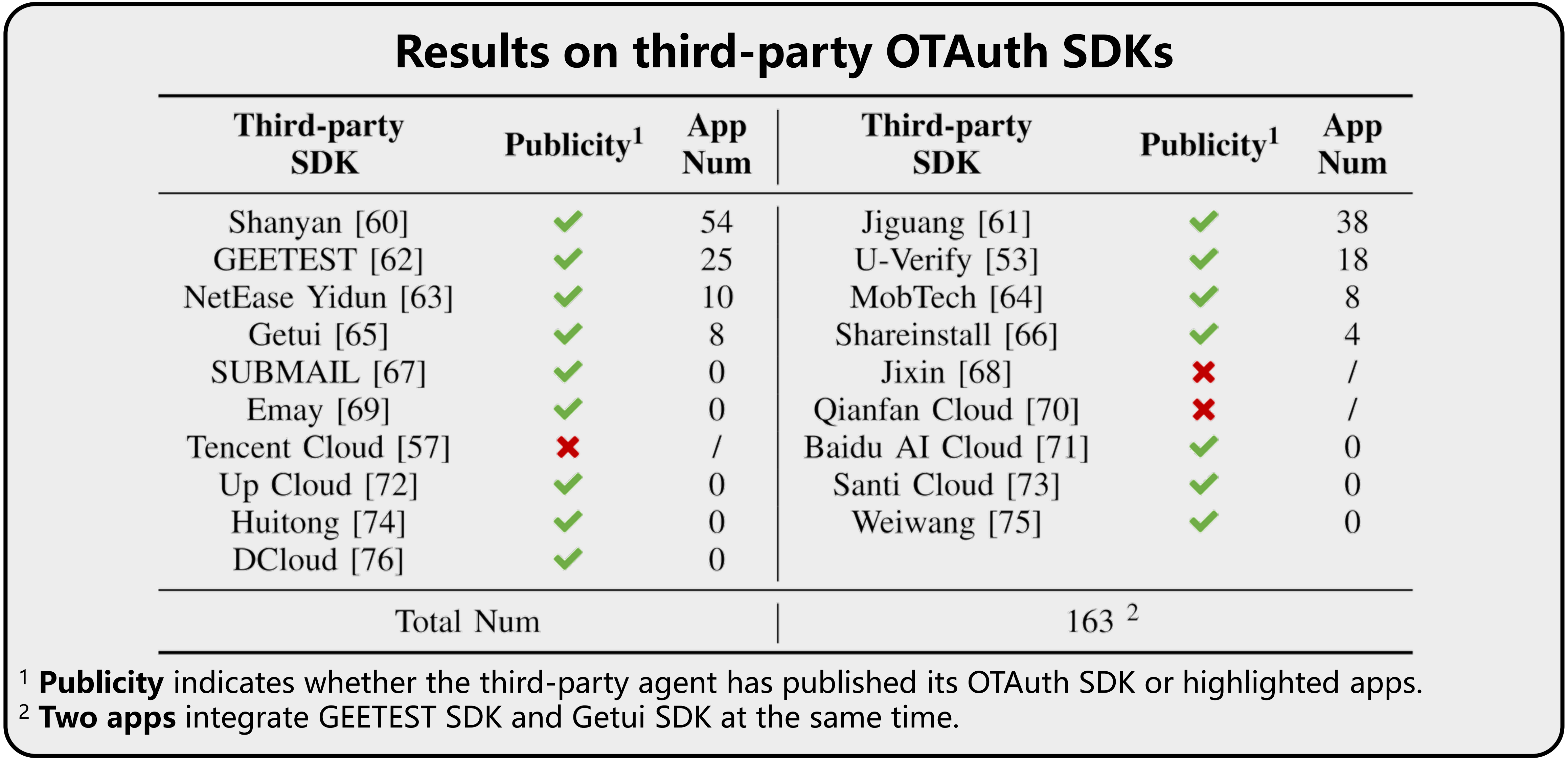


App	Category	MAU*	App	Category	MAU*
TikTok	short video	578.85	Sina Weibo	community	311.60
Baidu Input	input method	569.46	WiFi Master Key	Wi-Fi	285.57
Baidu	mobile search	474.62	TouTiao	comprehensive information	265.21
Gaode Map	map navigation	465.27	Pinduoduo	integrated platform	237.26
Kuaishou	short video	436.50	Dianping	local life	156.63
Baidu Map	map navigation	379.58	DingTalk	office software	143.57
Youku	comprehensive video	367.19	Meitu	picture beautification	139.47
Iqiyi	comprehensive video	350.90	Moji Weather	weather calendar	122.61
Kugou Music	music	321.29			

* MAU refers to the amount of Monthly Active Users (in millions).

Results and Findings

- **Affected SDKs**



Results on third-party OTAuth SDKs

Third-party SDK	Publicity[1]	App Num	Third-party SDK	Publicity[1]	App Num
Shanyan [60]	✓	54	Jiguang [61]	✓	38
GEETEST [62]	✓	25	U-Verify [53]	✓	18
NetEase Yidun [63]	✓	10	MobTech [64]	✓	8
Getui [65]	✓	8	Shareinstall [66]	✓	4
SUBMAIL [67]	✓	0	Jixin [68]	✗	/
Emay [69]	✓	0	Qianfan Cloud [70]	✗	/
Tencent Cloud [57]	✗	/	Baidu AI Cloud [71]	✓	0
Up Cloud [72]	✓	0	Santi Cloud [73]	✓	0
Huitong [74]	✓	0	Weiwang [75]	✓	0
DCloud [76]	✓	0			
Total Num			163 [2]		

[1] **Publicity** indicates whether the third-party agent has published its OTAuth SDK or highlighted apps.

[2] **Two apps** integrate GEETEST SDK and Getui SDK at the same time.

Results and Findings

- **Security Risks**

  □ **Unauthorized login as the victim user**

Results and Findings

- **Security Risks**

□ **Unauthorized login as the victim user**

□ **Account registration without user's awareness**

- If the used phone number has not yet been registered to the app service, it will be **automatically registered** without any user involvement.
- If the victim' phone number has not been used for registration, the attacker can register a new account with the victim's phone number.

Results and Findings

- **Security Risks**

□ **Unauthorized login as the victim user**

□ **Account registration without user's awareness**

□ **User identity leakage**

- Some app servers will send the **phone number** to the **app client**.
- Such an app server can be easily abused as an **oracle** to obtain the victim's phone number.

Results and Findings

- **Security Risks**

  - □ **Unauthorized login as the victim user**
  - □ **Account registration without user's awareness**
  - □ **User identity leakage**
  - □ **OTAuth service piggybacking**
    - To use OTAuth service, developers are required to register their apps and **pay the corresponding fees**.
    - A malicious app can use the *appId* and *appKey* of the victim app to obtain a token; then use this token to **exchange phone number** from **the app server**.

Results and Findings

- **Other Implementation Weaknesses**

Results and Findings

- **Other Implementation Weaknesses**
  - □ **Insecure token usage**
    - Token **reuse**
    - **Multiple effective** tokens
    - Too long **validity period**

Results and Findings

● **Other Implementation Weaknesses**

□ **Insecure token usage**

- Token **reuse**
- **Multiple effective** tokens
- Too long **validity period**

□ **Authorization without user consent**

- Some real-world apps have retrieved the token **before popping up the interface**

Results and Findings

- ● **Other Implementation Weaknesses**

  - □ **Insecure token usage**
    - Token **reuse**
    - **Multiple effective** tokens
    - Too long **validity period**

  - □ **Authorization without user consent**
    - Some real-world apps have retrieved the token **before popping up the interface**

  - □ **Plain-text storage of sensitive information**
    - Many real-world apps have **hard-coded** their *appId* and *appKey* into program files in plain-text form

Mitigation

- **Core idea**
  - Adding certain factors the malicious app cannot generate or cannot intercept

- **Countermeasures**
  - Adding user-input data into the login request
  - Adding OS-level support

Conclusion

- We uncovered several **design and implementation flaws of OTAuth**, which has a high popularity among real-world apps.

Conclusion

- We uncovered several **design and implementation flaws of OTAuth**, which has a high popularity among real-world apps.

- Exploiting the flaws of OTAuth scheme, we **designed an attack method** to **fully bypass** the authentication and perform malicious actions to the target app.

Conclusion

- We uncovered several **design and implementation flaws of OTAuth**, which has a high popularity among real-world apps.

- Exploiting the flaws of OTAuth scheme, we **designed an attack method** to **fully bypass** the authentication and perform malicious actions to the target app.

- We **evaluated the impact** of these threats. Our results showed that a large portion of **highly popular apps** are **vulnerable** to the attacks (38.6% for Android and 44.5% for iOS, respectively).

Thank you for watching