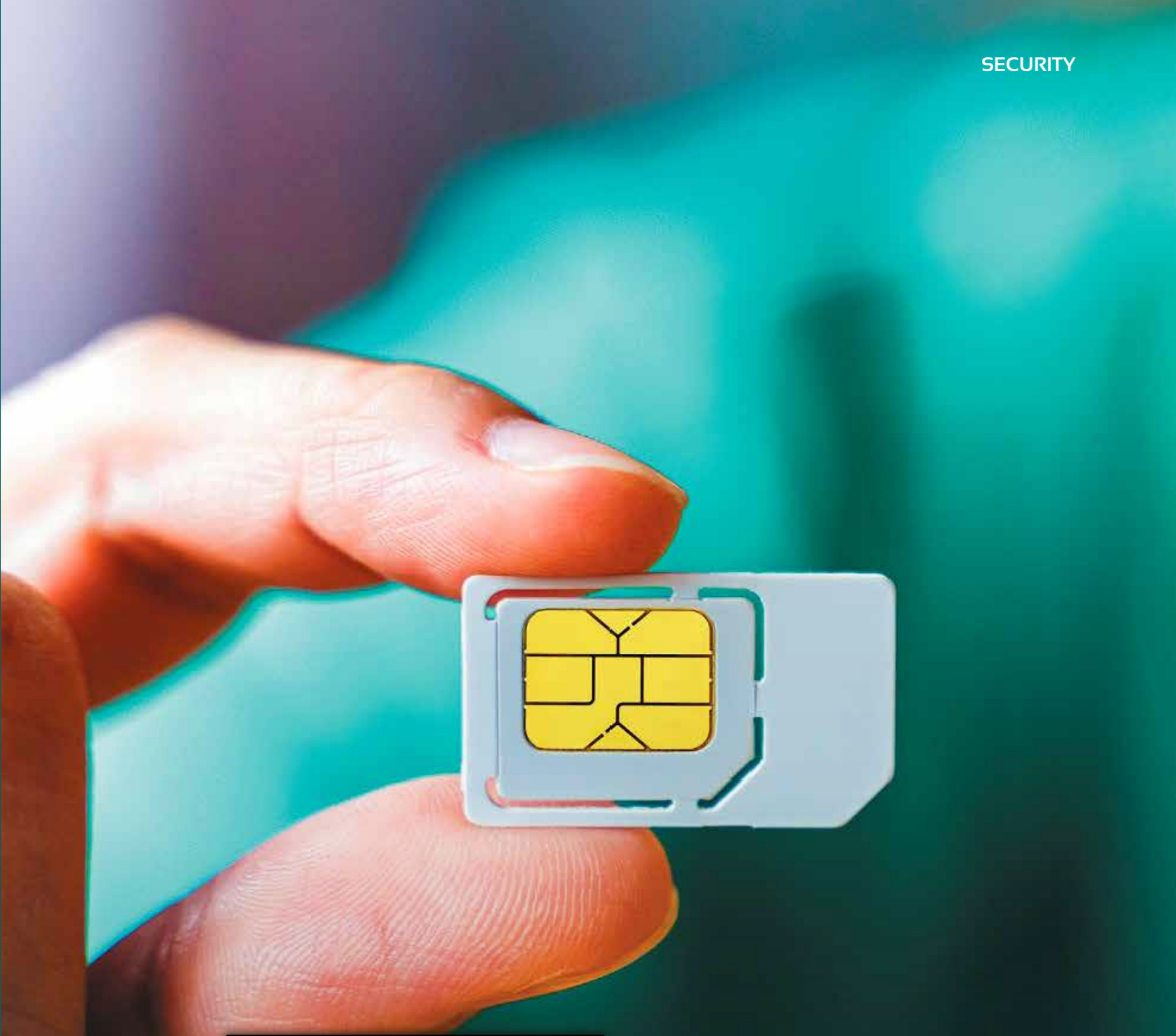

# ATTACCO SIM SWAP: LA NUOVA DELIBERA AGCOM E BUONE PRATICHE PER RIDURRE GLI IMPATTI

**ENISA - Countering SIM-Swapping**
Overview and good practices to reduce the impact of SIM-Swapping Attacks - Dec.r 6, 2021.
**AGCOM - Delibera n. 86/21/CIR**
Modifiche e integrazioni della procedura di portabilità del numero mobile, di cui alla delibera n. 147/11/CIR, e connesse misure finalizzate ad aumentare la sicurezza nei casi di sostituzione della SIM (SIM swap).

**di Giovanni NAZZARO**, *Lawful Interception Consultant, Security Manager, Auditor/Lead Auditor* ISO 27001, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni da 20 anni, esperto in *security*, *legal* e *compliance* in tali ambiti. Esperto nella progettazione dei sistemi d'intercettazione e di *data retention* e nella definizione delle procedure organizzative ed operative per il loro utilizzo. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della "*Lawful Interception Academy*" dal 2014, promotore della *LIA Certification* per la certificazione dei sistemi d'intercettazione. E' professore a contratto in Master Universitari di I e II livello.

Per un qualunque utente di telefonia mobile, che sia servito da un operatore americano, europeo o asiatico, lo scambio o la sostituzione di SIM, c.d. SIM Swap, è una procedura legittima eseguita per cambiare la propria SIM quando questa è stata smarrita, danneggiata o rubata, quando è necessario passare ad un altro formato di carta SIM oppure quando si effettua la portabilità del numero mobile.
Un attacco riuscito di SIM Swap effettuato da un malintenzionato, invece, abusa della capacità dell'operatore di espletare tale procedura, di conseguenza il proprietario legittimo della SIM vedrà disattivata la sua SIM e svuotarsi il proprio conto corrente in quanto il truffatore, ricevendo le chiamate e gli SMS al posto suo, potrà aggirare il doppio fattore autenticazione utilizzato dalle banche online.

Generalmente questo tipo di attacco si attua perché il malintenzionato studia la propria vittima tramite le informazioni che pubblica sui social networks e, sfruttando l'inconsapevole complicità dell'operatore mobile che adotta procedure standard o regolamenti nazionali, chiama il personale del call center e dichiara, spacciandosi per il vero intestatario del numero mobile, che è sua intenzione cambiare la SIM.

## 1. Il recente attacco a T-Mobile

Verso la fine di dicembre 2021, la multinazionale tedesca di telecomunicazioni T-Mobile, che offre i suoi servizi in diversi paesi del mondo tra cui Germania e Stati Uniti, ha confermato una violazione di dati collegata a notifiche inviate a un numero molto ridotto di clienti vittime di attacchi di SIM Swap. La notizia è arrivata tramite documenti interni condivisi con The T-Mo Report[1]. In realtà, negli ultimi quattro anni, T-Mobile è stata già vittima di molteplici violazioni dei dati, inclusa una molto simile nel febbraio 2021 quando gli aggressori hanno utilizzato un'applicazione T-Mobile interna per colpire fino a 400 clienti nei tentativi di scambio di SIM.
T-Mobile ha poi affermato che l'attacco è stato mitigato e che il problema è stato corretto, ma la società non ha fornito dettagli specifici sul numero di clienti interessati, né su come gli hacker sono stati in grado di eseguire gli attacchi di scambio di SIM. Ad esempio, non è escluso che gli hacker abbiamo avuto accesso alla **seconda categoria di dati,** oltre a quelli relativi alla SIM necessari per la sostituzione, rappresentati dalle **Customer Proprietary Network Information (CPNI),** informazioni riservate sull'acquisto e l'utilizzo di servizi di telecomunicazione da parte di un cliente, come le tipologie e le quantità di prodotti e servizi di telecomunicazione acquistati dal cliente oppure dettagli sulle chiamate effettuate (Call Data Records), quindi informazioni anche sulla posizione e sulla fatturazione con gli importi addebitati.

## 2. La situazione in USA

Uno studio accademico dell'Università di Princeton[2], pubblicato nel 2020, ha scoperto che i cinque principali operatori mobili prepagati statunitensi sono vulnerabili agli attacchi di SIM Swap. Secondo il team di ricerca, gli operatori AT&T, T-Mobile, Tracfone, US Mobile e Verizon Wireless utilizzano procedure vulnerabili con i loro centri di assistenza clienti, procedure che gli hacker potrebbero utilizzare per condurre attacchi di scambio di SIM. Si noti che T-Mobile era stata analizzata dagli studiosi un anno prima dei due ultimi attacchi di SIM Swap.
Cosa hanno fatto gli accademici di Princeton per dimostrarlo? Hanno passato il loro tempo chiamando i rispettivi call center degli operatori per vedere se potevano indurli a cambiare la SIM di un utente con un'altra, senza fornire le credenziali appropriate. Il team di ricerca ha applicato una procedura simile a quella mostrata in figura 1.

L'idea di base allo schema riportato è che l'attaccante chiami il call center per richiedere un cambio della carta SIM, fornendo "intenzionalmente" un PIN errato e dati relativi all'intestatario diversi, affermando di non ricordare quali informazioni aveva usato durante la registrazione della SIM. A questo punto, dopo aver fallito i primi due meccanismi di autenticazione (PIN e dati dell'intestatario), gli operatori di call center sono tenuti, in base alle loro procedure, a passare ad un terzo meccanismo durante il quale chiedono all'intestatario di fornire dettagli sulle ultime due chiamate fatte di recente.

Il team di ricerca afferma che, prima di un tale attacco, il malintenzionato potrebbe indurre una vittima a chiamare numeri specifici. Ad esempio, utilizzando una scusa come "hai vinto un premio; chiama qui; scusa, numero sbagliato; chiama qui invece". Dopo che l'attaccante

1. https://tmo.report/2021/12/t-mobile-has-suffered-yet-another-data-breach/

2. https://www.issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf

ha indotto con l'inganno il proprietario della carta SIM a effettuare queste due chiamate, può utilizzare questi dettagli per chiamare il call center della società di telecomunicazioni ed effettuare uno scambio di SIM.

## 3. Le linee guida di FBI

Un anno prima dello studio di Princeton, più precisamente a marzo 2019, il Federal Bureau of Investigation (FBI) aveva condiviso pubblicamente alcune linee guida[3] sulla difesa di questo tipo di attacchi, proprio a seguito di un preoccupante aumento del numero di attacchi di SIM Swap rivolti a investitori di criptovalute e intestatari di conti in valuta digitale. A novembre 2021 è stato registrato il più grande furto di criptovalute grazie ad un attacco di SIM Swap, perpetrato da un adolescente canadese che ha rubato $ 36,5 milioni in criptovaluta da una singola vittima statunitense[4].

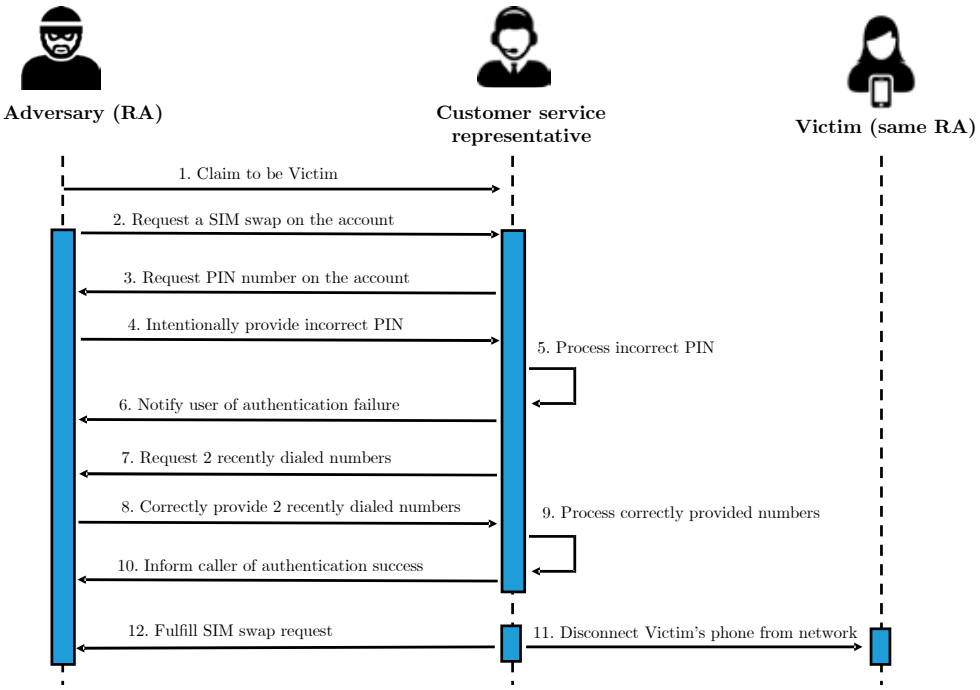


**Figura 1 - Procedura utilizzata dagli accademici di Princeton**

I criminali prendono di mira le vittime utilizzando le informazioni trovate sui *social media*, per questo l'FBI ha raccomandato di adottare le seguenti misure per evitare di diventare una vittima (anche se, occorre dirlo, nessuna guida è garantita per fermare questi attacchi):

- evitare di pubblicare dati personali online, come il numero di cellulare, l'indirizzo o altre informazioni personali; non lasciare documenti o informazioni importanti nella casella di posta elettronica (ad es. chiavi private in valuta digitale, documenti con il tuo numero di previdenza sociale o fotocopie della patente di guida);
- evitare di pubblicare informazioni online sulle risorse finanziarie (inclusa la criptovaluta), in particolare su qualsiasi sito Web e forum di social media;
- inserire un PIN sul proprio account associato alla numerazione mobile, affinché solo le persone con il PIN siano in grado di apportare modifiche all'account;
- usare password univoche, preferibilmente passphrase, e non riutilizzare la stessa password in ogni account;
- utilizzare app di autenticazione a due fattori o chiavi di sicurezza fisiche anziché SMS.

In caso si sospettasse di essere vittima di uno scambio di SIM, l'FBI consiglia di accedere al proprio account online per visualizzare le attività recenti ed insolite, di chiamare la propria banca segnalando tentativi di accesso probabilmente fraudolenti, infine di segnalare l'incidente alle forze dell'ordine.

## 4. Le buone pratiche consigliate da ENISA

Attraverso il rapporto di ENISA "Countering SIM-Swapping"[5], pubblicato il 6 dicembre 2021, l'Agenzia dell'UE per la sicurezza informatica ha fornito una misura in cui gli Stati membri sono interessati dagli attacchi di SIM Swap, elencando anche una serie di raccomandazioni come guida per le autorità nazionali, gli operatori, le banche e i cittadini.

In Europa il numero di incidenti di scambio di SIM varia notevolmente tra i paesi. In alcuni come Francia, Svizzera, Regno Unito, sono stati segnalati oltre 50 casi di scambio fraudolento di SIM per singolo operatore mobile (MNO), mentre in altri paesi gli operatori non hanno segnalato affatto frodi di SIM Swap come Austria, Croazia, Cipro, Lussemburgo, Romania, Slovacchia, Slovenia. Per l'Italia hanno partecipato quattro operatori mobile, di cui uno ha segnalato oltre 50 casi di SIM Swap (figura 2).

Tra le iniziative lanciate in tutta Europa per contrastare questo tipo di attacco, il rappor-

3. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-the-public-of-the-dangers-of-sim-swapping

4. https://www.bloomberg.com/news/articles/2021-11-17/canadian-teen-arrested-in-crypto-theft-worth-36-5-million

5. https://www.enisa.europa.eu/publications/countering-sim-swapping/@@download/fullReport

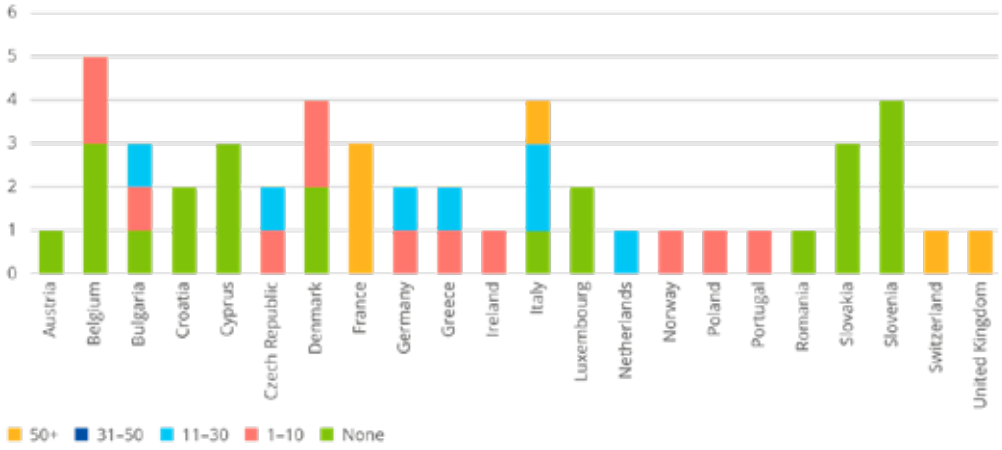


**Figura 2 - Distribuzione del volume degli attacchi di SIM Swap per paese/operatore**

to di ENISA prende a riferimento anche quello sperimentato in Italia, nel quale le banche hanno utilizzato una *application programming interface* (API) ovvero un'interfaccia fornita dagli operatori mobili (MNO) per verificare un recente scambio di SIM.

A fine 2018, infatti, grazie al supporto di Banca d'Italia e AGCOM (Autorità per le Telecomunicazioni), è stato creato un tavolo di lavoro congiunto tra CERTFin (CERT Finanziario Italiano) e gli operatori di telefonia mobile italiana, con l'obiettivo di avviare una sperimentazione su possibili contromisure tecniche. Tali attività sono state coordinate dal Comitato Tecnico Antifrode per le telecomunicazioni, composto dagli Operatori Nazionali aderenti alla procedura interoperatore di contrasto delle frodi scaturita dai lavori del tavolo tecnico ex art. 6 delibera AGCOM 418/07/CONS. L'Obiettivo del Comitato Tecnico Antifrode è di ridurre e prevenire le cause delle frodi, trasformare le attività in esperienza, monitorare l'efficacia del processo di cooperazione antifrode, assicurarne l'adeguamento/evoluzione nel tempo e mettere in comune le esperienze per una valutazione e riflessione da parte degli operatori afferenti.
L'idea di base al processo sperimentato è molto semplice ovvero coinvolgere gli MNO affinché avvisino le banche di un SIM Swap, che generalmente è la conclusione di una procedura lecita, tramite l'IMSI dell'abbonato oppure inviando informazioni sull'ora dell'ultimo cambio SIM.

In sintesi, l'API funziona come segue (figura 3):
1. il cliente avvia un trasferimento di fondi sulla propria App di *mobile banking* o da un computer;
2. la banca interroga il *database* dell'MNO del cliente tramite un'API;
3. l'MNO del cliente verifica se di recente si è verificato uno scambio di SIM sulla numerazione mobile (MSISDN) del cliente. In alternativa la banca fissa la soglia temporale (es. 24 ore) e l'MNO risponde se si è verificato uno scambio di SIM in un tempo inferiore alla soglia di temporizzazione.
4. se non è stato rilevato alcun cambio SIM recente sull'MSISDN del cliente, l'MNO del cliente comunica questa informazione alla banca come risposta all'API. Se è stato rilevato un recente scambio di SIM sull'MSISDN del cliente, l'informazione è inviata dall'MNO alla banca e questa esegue ulteriori controlli al fine di autorizzare la transazione;
5. la banca può procedere con il bonifico seguendo la procedura propria (es. inviando un SMS OTP al cliente).

Oltre all'utilizzo di un'API, sono state prese in considerazione anche altre due alternative:
- l'MNO invia alla banca la marca temporale dell'ultimo SIM Swap tramite il protocollo SMPP, dopo aver ricevuto apposita richiesta dalla stessa;
- l'MNO fornisce l'IMSI (o IMSI con hash) del cliente, utilizzando il protocollo standard SS7/MAP.

La soluzione principale e le sue due declinazioni tecniche presentano, ognuna, vantaggi e svantaggi. Ad esempio, con la soluzione con API non è richiesto che la banca conservi gli IMSI degli utenti, ma l'API deve essere utilizzata in tempo reale e quindi deve offrire livelli di servizio molto alti. Negli altri due casi, rispettivamente, si ha invece uno sviluppo tutto a carico dell'operatore nel caso del protocollo SMPP e tutto a carico della banca nel caso di invio dell'IMSI da parte dell'operatore, in quanto la banca dovrà costruire un *data base* locale con gli IMSI dei suoi clienti per confrontare la nuova informazione con quelle precedentemente memorizzate.

## 5. La delibera AGCOM n. 86/21/CIR

Come da comunicato stampa dell'AGCOM dell'8 luglio 2021[6], la Commissione Infrastrutture e Reti ha modificato dopo 10 anni la precedente delibera n. 147/11/CIR[7] introducendo

6. https://www.agcom.it/documents/10179/23560628/Comunicato+stampa+08-07-2021/ecbe8d11-6e6e-4ea6-be98-ad7a78275f39?version=1.0

7. https://www.agcom.it/documents/10179/539699/Delibera+147-11-CIR/48b1ed48-75dc-4362-9e43-e9ef6cf42230?version=1.0

meccanismi di prevenzione e di contrasto a eventuali tentativi di truffa a danno degli utenti finali di telefonia mobile, modificando il processo di portabilità e introducendo notifiche che garantiscono l'aggiornamento sullo svolgimento di eventuali attività di sostituzione della SIM che, quindi, l'utente sarà in grado di confermare o meno.

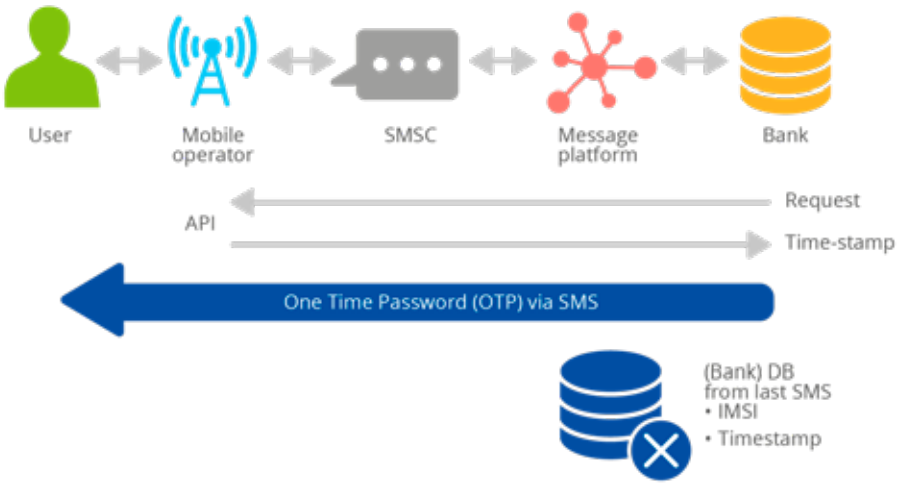


**Figura 3 - Processo di controllo tramite API per una transazione bancaria legittima**

La nuova delibera 86/21/CIR[8] segue la fase di consultazione pubblica, inerente alla delibera n. 334/20/CIR[9] del 19 novembre 2020, alla quale hanno partecipato 9 fornitori di servizi di comunicazione elettronica e tre associazioni dei consumatori, i cui esiti sono stati inseriti nell'allegato 1[10] della nuova delibera. Vediamo le principali novità, ricordando che la nuova delibera dovrà essere recepita entro 12 mesi dalla sua pubblicazione quindi entro luglio 2022.

L'art. 1 stabilisce che il titolare della SIM è l'unico soggetto che può richiedere il cambio SIM (co.1) inclusi i casi di richiesta di *Mobile Number Portability* (MNP), di furto o smarrimento, o altre fattispecie di modifica virtuale (eSIM), con la particolarità che "in caso di furto, smarrimento o malfunzionamento la richiesta della nuova SIM può essere effettuata solo presso il proprio operatore" e la richiesta di MNP può essere effettuata solo dopo aver sostituito la SIM (co. 2). La delega è consentita solo per le SIM aziendali e limitatamente ai casi che saranno declinati nell'ambito del Tavolo tecnico sulla MNP (co.3).

L'art. 2 tratta dell'identificazione dell'intestatario che dovrà avvenire secondo le norme vigenti e preventivamente al caricamento del profilo in caso di eSIM (co.1). L'operatore dovrà acquisire dal titolare copia fotostatica chiara e leggibile: i) del documento d'identità e di quello attestante il Codice Fiscale; ii) della vecchia SIM; iii) della relativa denuncia in caso di furto o smarrimento della SIM (co.2).

L'articolo 3 rappresenta il cuore delle novità introdotte dalla delibera per rafforzare la validazione del processo di sostituzione della SIM. Nei casi previsti, inclusa la MNP, l'operatore mobile deve effettuare sempre una validazione della richiesta inviando un SMS per informare il cliente che è stata richiesta la sostituzione della SIM e chiedendo conferma per proseguire (co.1). In alternativa, può acquisire la volontà del cliente chiamandolo e registrando la chiamata. Qualora non segua conferma all'SMS, il processo di sostituzione può proseguire esclusivamente nei seguenti casi: i) nel caso di SIM smarrita o rubata, qualora sia stata acquisita ed effettuata copia leggibile della denuncia all'Autorità competente e ii) nel caso di SIM guasta, qualora sia stata acquisita la vecchia SIM (co.2). L'articolo 6, comma 1, dell'**allegato 1** della delibera 147/11/CIR viene cambiato dalla delibera 86/21/CIR (*il testo dell'art. 3 co. 3 di quest'ultima non cita il riferimento all'allegato 1*), trasformando in obbligo l'invio dell'SMS da parte dell'operatore *recipient* per confermare la correttezza delle informazioni, quali il nome dell'operatore *donating* e *recipient* ed il numero principale con eventuali numeri addizionali da portare. Gli MNO devono prevedere una procedura semplice e di immediato utilizzo per l'utente al fine interrompere il processo se indesiderato (co. 4).
Infine, l'articolo 7 co. 2 stabilisce che il citato Comitato Tecnico Antifrode (ex delibera n. 418/07/CONS) confluisca nel nuovo Comitato tecnico sulla sicurezza delle comunicazioni elettroniche, coordinato dalla competente Direzione dell'Autorità, al quale possono partecipare, con un proprio rappresentante, anche il Nucleo Speciale per la Radiodiffusione e l'Editoria della Guardia di Finanza e la Sezione di Polizia Postale e delle Comunicazioni che collaborano con l'Autorità. ©

8. https://www.agcom.it/documents/10179/23529996/Delibera+86-21-CIR/dda35b70-5ea4-4f8d-9fef-06b0f4c1fe25?version=1.0

9. https://www.agcom.it/documents/10179/20606340/Delibera+334-20-CIR/d97d8e38-2e84-41c2-92af-04134d59d741?version=1.0

10. https://www.agcom.it/documents/10179/23529996/Allegato+27-7-2021/b1ddf8de-9dc1-4d1e-b0ae-fdd74757c36c?version=1.0