



# SecureCall Authorization

## Strong Authorization e Authentication

La soluzione a portata di mano, semplice come una telefonata,  
per garantire transazioni e accessi sicuri in completa mobilità



## L'evoluzione del mercato

Negli ultimi anni si è assistito ad una forte crescita del web e di servizi online basati su applicazioni che gestiscono dati personali e sensibili.

Questo trend deriva da molti fattori sia tecnici che economici. Tra questi, la disponibilità della banda larga, è certamente il fattore scatenante che ha permesso a molte aziende di offrire un maggiore numero di **servizi online** con la conseguente **riduzione dei costi operativi** e l'**incremento del livello qualitativo dei servizi** rivolti ai clienti.

**Le istituzioni bancarie e finanziarie** oggi sono le maggiori protagoniste in questi settori realizzando il maggior numero di nuovi servizi online. Tuttavia questa nuova frontiera ha innescato una **crescita parallela delle frodi IT** come phishing, pharming, man in the middle e man in the browser, causando rilevanti problemi sia per chi utilizza i servizi, sia per chi li offre.

Pertanto **nuovi sistemi di sicurezza** sono diventati necessari per **proteggere l'identità** personale durante tutte le transazioni.

Ad oggi, il sistema più diffuso per il controllo degli accessi ai servizi online è la strong authentication attraverso l'uso di token fisici dedicati.

SecureCall Suite è la soluzione ideale per la strong authentication, utilizzando lo strumento più diffuso e la più vasta infrastruttura esistente.

**Quale** è il prodotto elettronico di largo consumo più diffuso?  
**Quale** è il prodotto elettronico con lo standard più diffuso?  
**Quale** è il prodotto elettronico che identifica ognuno nella vita quotidiana?

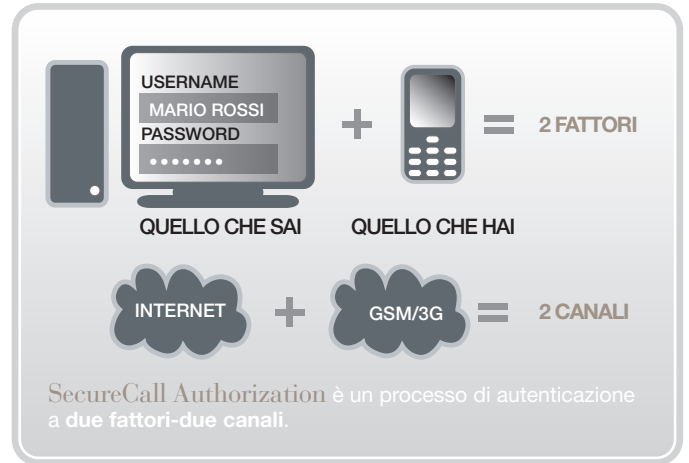
**Quale** è il "network" più diffuso e sicuro nel mondo?

I telefoni cellulari e le moderne reti mobili sono la risposta a tutte le precedenti domande.

# SecureCall Authorization

**SecureCall Authorization** è la soluzione che consente di utilizzare il telefono cellulare come **TOKEN** per certificare e abilitare le proprie credenziali richieste durante le fasi dispositive di tutte le transazioni sensibili online.

**SecureCall Authorization** utilizza un processo che combina **due fattori (PC e cellulare)** e **due canali per l'invio dei dati (web + rete Mobile)**. Questa modalità aggiunge un ulteriore livello di sicurezza e risolve efficacemente varie modalità di frodi informatiche, tra cui Man in the Middle/Browser, phishing e pharming. La soluzione, international patent pending, è ingegnerizzata per la prevenzione dello spoofing del cellulare.



## Come funziona

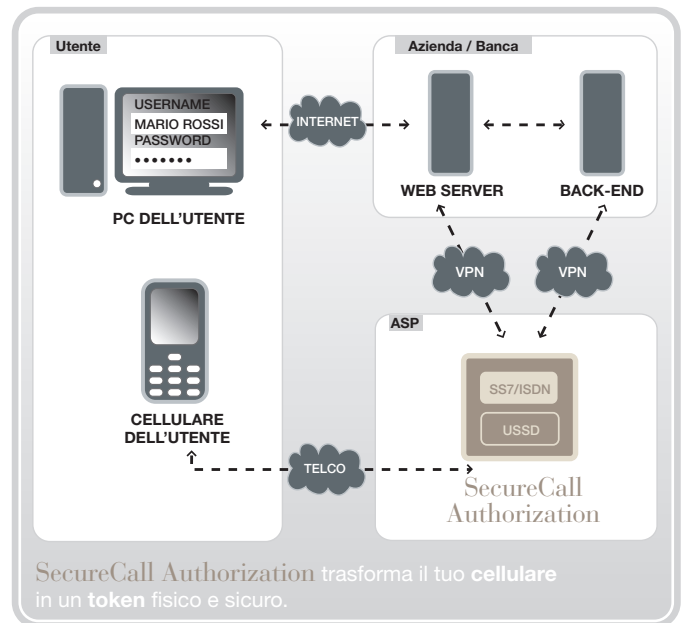
**SecureCall Authorization** consente agli utenti di autenticarsi utilizzando l'MSISDN del proprio cellulare (es 335.91234567), un numero univoco che identifica un utente appartenente ad una rete mobile.

La soluzione funziona con **qualsiasi apparato cellulare, non richiede l'installazione di alcuna applicazione** a bordo del telefono, SIM o PC e **non impiega OTP ricevute tramite SMS**; all'utente viene richiesto di effettuare una **SEMPLICE telefonata**.

**SecureCall Authorization** può essere usato per:

- **Autenticare** gli utenti per accedere ad aree riservate
- **Autorizzare** transazioni online
- **Effettuare** operazioni di Mobile Payment

**SecureCall Authorization** può essere implementata in House o in ASP presso il DataCenter di un carrier telefonico (soluzione raccomandata).



## Modalità di autenticazione

### Chiamata interrotta

Adatto per la gestione di un elevato numero di utenti a bassi costi di transazione



\*il servizio non genera alcun costo telefonico, la chiamata viene interrotta e pertanto non tariffata dal carrier telefonico

### Chiamata con DTMF PIN

Adatto per applicazioni che richiedono livelli di sicurezza maggiori



\*il servizio può generare del traffico telefonico con costi dipendenti dal piano tariffario del singolo utente = costo di una normale telefonata cellulare

### Chiamata in outbound

Adatto per applicazioni che richiedono il massimo livello di sicurezza delle transazioni e per un utilizzo all'estero



\*il servizio può generare del traffico telefonico con costi dipendenti dal piano tariffario del singolo utente = costo di una normale telefonata cellulare

# Vantaggi di SecureCall Authorization

## Comparazione tra i sistemi di autenticazione

	Autenticazione	Sicurezza	Economicità	Diffusione	Facilità	SLA
<b>Token</b>	Autenticazione con password numerica generata dinamicamente da un token dedicato sincronizzato con il server del sistema.					
<b>Smart card</b>	Autenticazione tramite firma digitale che viene custodita sul microchip di una smartcard leggibile da apposito lettore connesso al PC dell'utente.					
<b>OTP/SMS</b>	Autenticazione tramite password OTP ricevuta via SMS.					
<b>SecureCall Authorization</b>	Autenticazione tramite una semplice telefonata a SecureCall Authorization.					

SecureCall Authorization: il servizio di strong authentication **facile da usare e a portata di mano.**

### Vantaggi per le aziende

- Nessun costo di logistica e di gestione per i tokens
- Nessuna nuova procedura da insegnare al cliente
- Nessuna applicazione da scaricare e installare sul cellulare
- Nessun server e software da installare e mantenere
- Più sicurezza utilizzando la rete Mobile via SS7

### Vantaggi per gli utenti

- Nessuna possibilità di Phishing, Pharming, MiM e MiB
- Nessun OTP da ricevere via SMS
- Nessun software da installare sul cellulare
- Nessuna applicazione SIM richiesta
- Tutti i cellulari di tutti gli operatori mobili sono supportati

### Referenze

Telecom Italia  
Poste Italiane  
Cariparma (Crédit Agricole Group)  
Allianz  
Monte dei Paschi di Siena  
Consorzio Triveneto  
Banca Sella Group  
... e molti altri

Per maggiori informazioni [www.aliaslab.net](http://www.aliaslab.net)

Aliaslab s.p.a.

Uffici  
via Cremona 27/6 - 46100 Mantova - Italy  
Ph + 39 0376 285101 F + 39 0376 263856  
Sede legale  
via Durini, 25 - 20122 Milano - Italy  
[www.aliaslab.net](http://www.aliaslab.net)