TIME4ID

AUTENTICAZIONE MULTIFATTORE

Time4ID è una piattaforma di **Strong Authentication** interamente sviluppata da Intesi Group che risponde alle attuali esigenze di sicurezza del mercato italiano (ad esempio, SPID - Sistema Pubblico di Identificazione) e internazionale come PSD2 e BCE Recomandations per la sicurezza dei pagamenti online.

PROTEGGI LA TUA IDENTITÀ DIGITALE

TIME4ID

powered by **Intesi Group**
www.intesigroup.com

TIME4ID AUTENTICAZIONE MULTIFATTORE

MODALITÀ PUSH

Time4ID consente la **generazione di OTP** con dispositivi mobili (iOS e Android) tramite un'App personalizzabile o un SDK per integrazioni applicative mobile.
Sulla piattaforma Time4Mind, integrati con Time4ID, sono già disponibili anche i servizi di Firma Remota, naturale evoluzione della Strong Authentication.
Sia l'autenticazione che la firma sono fruibili in **modalità push**. L'utente riceve sul proprio smartphone una notifica con i dettagli dell'operazione da autorizzare, come ad esempio il login a un portale applicativo, una transazione o una firma elettronica. La risposta affermativa sblocca la generazione e l'invio della OTP dalla App al backend applicativo. Poiché in questo modo non è più necessario leggere e scrivere alcuna OTP, con Time4ID si ottengono il massimo della semplicità di utilizzo e della sicurezza.

OUT-OF-BAND

In particolare, poiché lo smartphone utilizza una linea dati distinta (out-of-band) rispetto a quella del servizio applicativo, con la **push authentication** vengono fortemente mitigati gli attacchi di tipo phishing e man-in-the-middle. Inoltre, se l'operazione da effettuare lo richiede, è anche possibile da parte dell'utente l'immissione di alcuni dati, come ad esempio il PIN di sblocco della credenziale di firma remota, che viene trasmesso cifrato per garantire sempre la massima riservatezza.

ARCHITETTURA

L'architettura cloud PaaS consente di realizzare processi di registrazione e autenticazione con un DB utenti nativo o integrando quello del cliente. Time4ID supporta come transparent gateway anche altri sistemi di Strong Authentication hardware (Vasco, RSA, OATH, Radius, SMS e Grid card). L'architettura cloud è progettata per garantire business continuity, alta scalabilità e massima sicurezza grazie all'utilizzo di HSM per la cifratura dei dati presenti su DB.

Funzionalità push authentication / push signature / transaction authentication (OTP signature) / modalità out-of-band con logica push / supporto multitoken per usi differenziati / supporto multidevice con dispositivo Master + Backup / crittografia innovativa del seed su dispositivi mobili / protezione del seed con Hardware Security Module sul Backend / dati antifrode / device reputation / OTP nativi (Time4ID) e di terze parti (OATH, Gemalto, RSA, Vasco, CA, Asseco, Radius, SMS) possono essere usati in modo trasparente per le applicazioni