TIME4ID

THE UNEXPECTED STRONG AUTHENTICATION

Time4ID is a **Strong Authentication** platform entirely developed by Intesi Group that meets current security requirements by the Italian (for example, SPID - Public Digital Identity System) and international markets (for example, “ECB recommendations for the security of Internet payments”).

IT’S NOBODY ELSE, BUT YOU.
Protect your digital identity.

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

TIME4ID

THE UNEXPECTED
STRONG AUTHENTICATION

ver. 09/2016

PUSH NOTIFICATION

Time4ID allows **OTP generation** with mobile devices (iOS, Android and Windows Phone) via a customizable App or a SDK mobile application integration. On the Time4Mind platform, integrated with Time4ID, the Remote Signature Services are available as the natural evolution of Strong Authentication.
Both authentication and signature are usable in **push mode**. The user receives a notification on his smartphone with details of the transaction to be authorized, as a log in to a portal application, a transaction or an electronic signature.

OUT-OF-BAND

The affirmative answer unlocks the OTP generation and its trasmission from the App to the backend application. Since in this way is no longer necessary to read and write any OTP, Time4ID allows the best security and ease of use.
Especially with **push authentication**, phishing and man-in-the-middle attacks are strongly mitigated, since the smartphone uses a separate data line (out-of-band) than to the application service. Furthermore, it's also possible by the user to enter data, such as the unlock PIN for remote signature credentials, which is transmitted encrypted to protect the maximum confidentiality.

ARCHITECTURE

The cloud PaaS architecture allows creating registration and authentication processes with a native user DB or integrating an existing one. Time4ID is a transparent gateway that also supports other Strong Authentication hardware (Vasco, RSA, OATH, Radius, SMS and Grid card). The cloud architecture is designed to ensure business continuity, high scalability and maximum security thanks to the use of HSM to encrypt data on DB.

Features out-of-band mode with push notification / explicit OTP / implicit OTP / transaction authentication (OTP signature) / multitoken support for different uses / multidevice support with Master device + Backup / innovative seed encryption on mobile devices / seed protection with Hardware Security Module on backend / antifraud data / device reputation / encrypted communication channels / data center ISO27001 with high availability and disaster recovery