TIME4ID

THE UNEXPECTED STRONG AUTHENTIFICATION

Time4ID is a **Strong Authentication** platform, entirely developed by Intesi Group, that meets the current security requirements of the Italian and international markets (for example, SPID - Public Identification System) and international needs such as PSD2 and BCE Recomandations for online payment security.

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

TIME4ID

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

ver. 11/2019

TIME4ID THE UNEXPECTED STRONG AUTHENTIFICATION

PUSH NOTIFICATION

Time4ID allows **OTP generation** with mobile devices (iOS and Android) 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 available in **push mode**. The user receives a notification on his smartphone with the details of the transaction to be authorized, such as login to portal an application, a transaction or an electronic signature. In this way it isno more necessary to read and write any OTP. With Time4ID you have a simple and safe experience.

OUT-OF-BAND

The smartphone uses a different (out-of-band) data line to the one used by application service. With push authentication phishing and man-in-the-middle attacks are strongly mitigated. Moreover, if required it is possible to enter some data, such as for example the PIN for unlocking the remote credential, which is transmitted encrypted to guarantee always the utmost confidentiality.

ARCHITECTURE

The cloud PaaS architecture allows the creation of 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 systems (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 HSMs to encrypt data on DB.

Features push authentication / push signature / transaction authentication (OTP signature) / out-of-band mode with push mode / multitoken support for different uses / multidevice support with Master + Backup / immovative encryption of the seed on mobile devices / seed protection with Hardware Security Module on the Backend / anti-fraud data / device reputation data