Mobile App Security

At Salto, we believe that security should be a top priority when it comes to mobile applications. We understand that users today are increasingly concerned about the security and privacy of their personal information, and we take this concern seriously. That's why we have implemented various security features aligned with international standards like OWASP MASVS in our mobile applications to ensure that your personal information is kept secure and protected at all times.

One of the essential security features that we prioritise is a secure architecture and design. Our mobile applications are designed with multiple layers of security, which prevent attackers gaining access to sensitive data and information. Our design approach ensures that any vulnerabilities in the application's architecture are identified and addressed before deployment. Moreover, we use secure data storage mechanisms that encrypt your data both in transit and at rest, using strong cryptographic algorithms. This ensures that your personal information is protected from unauthorised access and breaches.

Authentication and sessions are equally crucial security features that we implement in our applications. We use secure authentication and session management techniques to protect your data from illegitimate access and ensure your session remains secure. Likewise, we use secure communication protocols to protect your data during transmission. Similarly, we implement data privacy controls, which give control over personal data and how it's used.

Additionally, we interact with our platforms using secure communication channels and use secure coding practices to prevent unauthorised access to our source code, as well as making sure that our code remains secure against any threat.

Disclaimer:

salto /\
INSPIRED ACCESS