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:

This is a downloadable version of the website content that we make available to you for informative purposes for an easier consultation and filling. However, Salto assumes no responsibility for any errors or typos that the downloadable version may contain.

Part of the content of this document may have been generated or assisted by artificial intelligence tools. This document may also include automatic or manual translations provided exclusively for informational purposes, which may contain errors or inaccuracies. Salto does not guarantee the accuracy, quality, or reliability of such content or translations, including those generated by AI.

The User is responsible for verifying the information contained in this document and, in case of doubt, must refer to the original English version, which shall prevail in the event of any discrepancy. Other language versions are provided for informational purposes only.

Although Salto makes reasonable efforts to review the content of its downloadable documents, they may contain errors or omissions. Salto assumes no liability arising from the User's use, interpretation, or decisions made based on the information contained in this document, which is used at the User's sole responsibility.

For more detailed information on the use of artificial intelligence, translations, and applicable limitations of liability, please refer to the "Terms of Use of our Website".

As Salto reserves the right to modify this content from time to time, please check on the Legal section of our website to find the latest version of the legal documents and their updates.

Copyright ©2026 SALTO Systems S.L. All rights reserved