ZIMPERIUM®

How Zimperium's MAPS Capabilities Help Ensure Compliance with PSD2 Regulatory Standards

The Payment Service Directive 2 (PSD2) is a European regulation for electronic payment services. See how Zimperium's Mobile Application Protection Suite (MAPS) can help financial institutions comply.

Article	Title	Requirement Description	App Hardening zSHIELD™	Runtime Protection zDEFEND™
2	**General Authentication Requirements**	2. (d) signs of malware infection in any sessions of the authentication procedure;		✓
6	**Requirements of the elements categorised as knowledge**	1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties. 2. The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.	✓	✓
7	**Requirements of the elements categorised as possession**	1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties. 2. The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.	✓	✓
8	**Requirements of devices and software linked to elements categorised as inherence**	1. Payment service providers shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the payment service providers shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.		✓

Article	Title	Requirement Description	App Hardening zSHIELD™	Runtime Protection zDEFEND™
9	**Independence of the elements**	1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements. 2. Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised. 3. For the purposes of paragraph 2, the mitigating measures shall include each of the following: a) the use of separated secure execution environments through the software installed inside the multi-purpose device; b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party; c) where alterations have taken place, mechanisms to mitigate the consequences thereof.	✓	✓
18	**Transaction risk analysis**	2. i) unusual information about the payer's device/ software access; ii) malware infection in any session of the authentication procedure;		✓

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244