nextAuth compliance with PSD2 SCA

With the Payment Services Directive 2 (PSD2), the EU aims to reduce the risk of fraud in electronic payment services. Towards this goal it mandates the adoption of Strong Customer Authentication (SCA). The European Banking Authority's (EBA) wrote the Regulatory Technical Standard (RTS) for SCA. This document describes how nextAuth meets the relevant requirements.

How nextAuth meets the RTS requirements

REFERENCE	REQUIREMENT	COMPLIANCE
Article 2.2	Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors: (d) signs of malware infection in any sessions of the authentication procedure;	The nextAuth client implements application shielding, detecting amongst others root/jailbreak, hooking, debug and malware. This information is passed along to the nextAuth server and can serve as input to the payment service provider's risk analysis.
	(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.	The nextAuth server keeps a log of all authentications (login, transaction signature) performed by each nextAuth client (access software).
Article 4.1	[…] the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.	The authentication codes generated by the nextAuth client are cryptographic signatures, based on the elements of possession and knowledge and/or inherence.
Article 4.2	[…] payment service providers shall adopt security measures ensuring that each of the following requirements is met: (a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;	The authentication codes generated by the nextAuth client are cryptographic signatures. As such, these authentication codes: - do not reveal any information on the underlying authentication elements.

REFERENCE	REQUIREMENT	COMPLIANCE
	(b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;	- do not help to generate a new authentication code for any future authentication.
	(d) authentication code cannot be forged.	- cannot be forged.
Article 4.3	Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures: (a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code […], it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;	The information on the authentication elements that failed is not exposed.
	(b) the number of failed authentication attempts that can take place consecutively […] shall be temporarily or permanently blocked, shall not exceed five within a given period of time;	The nextAuth server implements a fail counter, which limits the PSU in entering an incorrect knowledge element in combination with a possession element, no more than three consecutive times after which the account is blocked. With respect to the inherence element, the biometric API's of the mobile OS enforce a temporary blocking mechanism in the number of failed attempts over time.
	(c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties […];	Authentication data are always transmitted over a dedicated secure channel between nextAuth Client and nextAuth Server.
Article 4.4	Where the block […] is temporary, the duration of that block and the number of retries shall be established based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors […] Where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.	After entering an incorrect knowledge in combination with a possession authentication element, the payer is alerted of the number of tries left. After a successful verification of the possession and inherence authentication elements (server-side), the account is unblocked (it is again possible to generate authentication codes based on possession and knowledge authentication elements). If this is not possible, the user will recover use of the blocked electronic payment instrument through re-activation, which follows the same procedures as the initial activation.

REFERENCE	REQUIREMENT	COMPLIANCE
Article 5.1	Where payment service providers apply strong customer authentication […] they shall also adopt security measures that meet each of the following requirements: (a) the payer is made aware of the amount of the payment transaction and of the payee;	The nextAuth client displays the amount of the payment transaction and the payee in the transaction approval screen to the payer.
	(b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;	The message that is cryptographically signed (authentication code) contains the amount of the payment transaction and the payee.
	(d) any change to the amount or the payee results in the invalidation of the authentication code generated.	The authentication code (cryptographic signature) becomes invalid for any change in the message that was signed.
Article 5.2	[…] payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following: (a) the amount of the transaction and the payee throughout all of the phases of the authentication;	The mutually authenticated secure channel established between the nextAuth server and the nextAuth client, and the generated authentication codes (digital signatures) by the nextAuth client, ensures the confidentiality, authenticity and integrity of the amount of the transaction and the payee.
	(b) the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.	The nextAuth client implements application shielding, protecting the confidentiality, authenticity and integrity of the information displayed to the payer. Furthermore, the nextAuth client also includes a screenshot of what is displayed to the user in the message to be cryptographically signed (authentication code) for the transaction, further protecting the integrity of the information displayed to the user.
Article 6.1	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.	The nextAuth client never transmits the PIN, instead it is combined with a possession element in such way that verification requires the assistance of the nextAuth server (preventing local brute-forcing) without the nextAuth server ever learning the PIN.
Article 6.2	The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.	The nextAuth client implements application shielding and its own PIN pad, which does not provide visual feedback on the buttons pressed, and masks the input, making sure that in the use of the PIN by the payer, it is not disclosed to unauthorised parties.
Article 7.1	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.	The nextAuth server has procedures to unlink lost and stolen mobile devices from the PSU.

REFERENCE	REQUIREMENT	COMPLIANCE
Article 7.2	The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.	The nextAuth client implements device binding, preventing the replication of the possession elements.
Article 8.1	Payment service providers shall adopt measures to mitigate the risk that the authentication elements categorised as inherence […]. 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.	The nextAuth client makes use of the biometric API's of the mobile OS to put a signature on a given message inside the mobile device's secure execution environment after successful verification of the inherence element.
Article 8.2	The use by the payer of those [inherence] elements shall be subject to measures ensuring that those devices and the software guarantee resistance against unauthorised use of the elements through access to the devices and the software.	The nextAuth client makes use of the biometric API's of the mobile OS to put a signature on a given message inside the mobile device's secure execution environment after successful verification of the inherence element.
Article 9.1	Payment service providers shall ensure that the use of the elements of strong customer authentication […] 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.	Compromise of the nextAuth possession elements does not lead to compromise of the knowledge element, and vice versa. Compromise of the inherence element affects neither the possession or the knowledge elements.
Article 9.3	*Payment service providers shall adopt security measures […] to mitigate the risk which would result from that multi-purpose device being compromised.* […] 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;	The nextAuth client creates a secure execution environment by relying on app separation as provided by the mobile OS combined with its implementation of application shielding. The secure execution environment for verification of the inherence factor is provided by the mobile OS.
	(b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;	The nextAuth client implements application shielding, detecting amongst others root/jailbreak, hooking, debug and malware.
	(c) where alterations have taken place, mechanisms to mitigate the consequences thereof.	The nextAuth client implements application shielding that can respond in different ways to detected alterations, ranging from alerting the nextAuth server (which can serve as input to risk analysis of the payment service provider) to shutting down the nextAuth client.

REFERENCE	REQUIREMENT	COMPLIANCE
Article 18.2	An electronic payment transaction […] shall be considered as posing a low level of risk where all the following conditions are met: (c) payment service providers as a result of performing a real time risk analysis have not identified any of the following […]	The nextAuth client implements application shielding, detecting amongst others root/jailbreak, hooking, debug and malware. This information, together with geographic information is passed along to the nextAuth server and can serve as input to the payment service provider's risk analysis.
Article 22.2	*Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.* [...] payment service providers shall ensure that each of the following requirements is met: (a) personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;	The nextAuth client masks the input of its custom PIN pad.
	(b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text;	The nextAuth client never stores personalized security credentials or cryptographic material related to the encryption of these credentials in plain text.
	(c) secret cryptographic material is protected from unauthorised disclosure.	The nextAuth client stores cryptographic material in the protected device store offered by the mobile OS or in encrypted format that is only accessible after a successful multi-party computation with the server.
Article 22.3	Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.	All processing of personalized security credentials and of authentication codes are done with the secure execution environment of the nextAuth client or the secure execution environment as provided by the mobile OS.
Article 22.4	Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards.	All processing of personalized security credentials and of authentication codes are done with the secure execution environment of the nextAuth client or the secure execution environment as provided by the mobile OS. All routing of authentication codes is done within the secure execution environment of the nextAuth client in accordance with strong and widely recognized industry standards.

REFERENCE	REQUIREMENT	COMPLIANCE
Article 23	Payment service providers shall ensure that the creation of personalised security credentials is performed in a secure environment. They shall mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.	The creation of personalized security credentials is performed within the secure execution environment of the nextAuth client or the secure execution environment as provided by the mobile OS (inherence element).
Article 26	Payment service providers shall ensure that the renewal or re-activation of personalised security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices […].	Re-activation follows the same procedures as the initial activation.
Article 27	Payment service providers shall ensure that they have effective processes in place to apply each of the following security measures: (a) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;	The nextAuth server can revoke each nextAuth client (and associated personalised credentials) by unlinking the nextAuth client from the PSU's identity. At this point, the personalised security credentials are rendered useless. This nextAuth server will instruct the nextAuth client to destroy the revoked credentials.

Conclusion

The nextAuth client for Android and iOS, together with the nextAuth server fulfils all requirements of the EBA's RTS on Strong Customer Authentication which are in scope of the product. nextAuth is a state-of-the-art solution, with its patented True Two-Factor Authentication, strong non-repudiation for transaction signing and an end-to-end mutually authenticated secure channel between the nextAuth client and nextAuth server.