Integration, hosting, security

Integration with Verestro

Verestro offers three ways to take benefit of our solution, see table below for detailed comparison and pros of each of them.

	White Label Application	**SDKs**	**APIs**
What is it?	Complete mobile application for Android & iOS. Ready to be branded, customized and deployed to your users.	Native development kits for Android & iOS. Libraries easily pluggable into your existing mobile app, they take care of heavy-lifting and allow you to focus on User Experience.	REST-based interface to enable integration of your existing back-end to our services.

Key benefits	• Shortest time to market - ready to deploy in 20 days. • Modular approach - pick what you need. • Field-tested UX and processes. • Well defined customization scope, to guarantee on-time delivery. • Open to extension - it's possible to add new modules specific to your business.	• Full flexibility in creation of User Interface • Device security, encryption, session management are taken care of - your development team needs to focus only on experience of your users. • Minimal impact on back-end. Our SDKs connect to our back-ends, limiting scope of the project on your end, mostly to mobile application.	• Seamless integration to all your existing services including mobile apps, web or any other platform like IoT or Wearables. • Mix and compose our solution with your existing processes to create familiar environment for your users, with no compromises. • Handling of sensitive data is still covered, using strong, yet easy to implement cryptography. According to current best industry standards.
When to choose?	• Your product is created from scratch. • Time to market is crucial. • Development impact on your organization has to be minimized.	• Mobile application already in-place. • Needs expansion with fin-tech functionality. • There's capacity for mobile development.	• Existing multi-channel solution. • Mobile app already present or not necessary. • Verestro API will be used to augment existing financial product. • There's capacity for back-end development on your side.

Sandbox Environment

We have sandbox environment available per request. Contact sales@verestro.com to get access.

More information about connection configuration can be found here: Connecting to server-to-server APIs.

Hosting

We deliver our products in Software-As-A-Service Model. We build a new instance of the platform for new customers and we host in either in private cloud (European Union) or public cloud (AWS anywhere in the world). We prefer this model of delivery as almost every software component is going through updates every 2nd week. We need to make sure service is compliant with security requirements, android, iOS, Mastercard, VISA so we are in a constant development process. It is usually impossible or very difficult to go through regular deployment and release process if we do not host the platform.

Security Standards and PCI DSS

Verestro is compliant with the highest level of PCI DSS Standards - Level 1. We are regularly going through system scans and once per year we are going through on-site audit performed by certified PCI DSS auditor. Verestro is also regularly checked and verified by Mastercard or VISA and multiple institutions (including big banks) that are regularly auditing Verestro infrastructure. We achieved the highest security standards by:

1. Building and maintaining network security - the need to build and maintain a firewall configuration that protects cardholder data, not using manufacturers' default passwords and settings.
2. Protecting cardholder data - protecting stored cardholder data, encrypting data transmissions when using public networks.
3. Maintaining a payment management program - using regularly updated anti-virus systems, developing secure systems and applications.
4. Implementing strong access control methods - limiting access to cardholder data to only those with a business need, assigning each user a unique ID, limiting physical access to cardholder data.
5. Regular network monitoring and testing - testing security systems and processes, controlling access to network resources and cardholder data.
6. Maintaining information security policies - relying on security policies for employees and vendors.

Revision #17
Created 21 June 2022 09:30:58 by Michał Maciąg
Updated 30 August 2023 14:56:35 by Michał Maciąg