rezolve
instant salesware

Rezolve Overview - Security

Version 1.9

rezolve
instant salesware

Contents

Introduction to Rezolve 3
Introduction to Security in Rezolve 3
Rezolve Security Philosophy: *Security built in*™ 4
User Authentication 4
Secure Connections Over Public Networks 4
Encryption of Data in Storage 4
Protection of Cardholder and Payment-related Data 5
Payment Processing 5
Protection of Personal Identifiable Information 5
Know Your Customer (KYC) and Anti-Money Laundering (AML) 5
Data Sharing 6
Security Architecture Summary 6

Introduction to Rezolve

Rezolve™ is a ground-breaking mobile-payments SDK and platform that allows banks, mobile network operators, retailers, media companies and other mobile consumer audience owners to deliver rich and engaging consumer experiences to their users. With the Rezolve Inside™ SDK embedded in a host mobile app, consumers can pay bills, top-up mobile devices, and shop for retail products and services with simple navigation and a 'scan-and-tap' on their mobile device. By combining the native capture mechanisms of the mobile device – camera, microphone and location awareness – with a mobile wallet and Rezolve's powerful merchant integration technologies, Rezolve turns any mobile device into an active engagement tool for shopping and for managing consumer mobility. The consumer's experience is intuitive, fast and secure, while Rezolve orchestrates all user flows, data flows, order creation and payments, integrating to merchant commerce platforms and payment providers as needed. With Rezolve Inside™, the host app owner benefits from new lines of consumer engagement and participates in transaction revenues, without having to develop code, host operations, or manage security.

Introduction to Security in Rezolve

Rezolve is committed to mobile security and privacy. The platform's technical design is based on future proof best-in-class models while maintaining simplicity and transparency for end users. Users' data privacy is safe-guarded with database and network encryption, role-based data access policies and other purposely designed security measures.

Security controls are designed into the platform from the ground up, from the front-end consumer mobile apps and web-based admin portals, through all data transport layers, to the back-end services, business logic services, databases, and internal and external APIs. The platform is supported by a robust infrastructure to mitigate against common and known threats, and the front-end apps and portals are protected by the physical possession of the mobile devices and user authentication challenges.

Rezolve Security Philosophy: *Security built in*™

Security is built into the Rezolve platform's technical architecture from the core, using the separation of concerns (SoC) principle. In the security context, the SoC principle is used to break secret and sensitive data into discrete sections and distribute them across the platform's services such that, in the unlikely event of any breach of individual services or even of multiple services, any data that might be exposed is incomplete and without context, and so is without value. As well as employing SoC principles at the code and data level, Rezolve also employs the principle at the business objects level, such that data pertaining to one party (for example a Merchant) is partitioned from the data pertaining to all other parties.

User Authentication

End users can be the weakest link in any security chain, so Rezolve observes Internet best practices for end user authentication; both for Consumer users accessing Rezolve-powered apps, and for Admin users accessing administration portals. Password and passcode security challenges are used across the user interfaces, users are encouraged to use strong passwords and passphrases and, in the case of mobile user interfaces, native mobile OS security measures can also be employed, for example biometric ID authentication. Host apps using the Rezolve Inside SDK can continue to use all their currently employed user authentication measures (for example biometric, voice recognition, passphrase, and two factor authentication) and securely hand-off users to the Rezolve user experiences (using *federated* user account), so that apps and web-based interfaces, for example banking apps that routinely employ the strongest authentication measures, can remain safe against unauthorized access.

Secure Connections Over Public Networks

Like most modern commerce, financial and banking apps and platform, some elements of the Rezolve platform's communications rely upon the public internet for transporting private and public data. Rezolve uses universally recognized and trusted strong encryption techniques for all such data, including using HTTPS (TLS 1.0) for all communications between apps, portals, back end platform, and external systems (e.g. Merchants and payment providers), with an additional level of payload encryption layered on top.

Encryption of Data in Storage

In the normal course of its operations, the Rezolve platform may store certain information about users, businesses, and other entities. In the case of users this includes personal information such as names, addresses, and email addresses, as well as payment method details, and in the case of businesses it may include product and pricing information, as well as payment service provider credentials. Rezolve protects data with strong encryption to industry certified standards (see PCI DSS) coupled with Rezolve's *Security built in*™ philosophy based upon SoC principles.

Protection of Cardholder and Payment-related Data

Payments and commerce platforms routinely handle cardholder and other payment-related data, and Rezolve is no exception. Security standards such as PCI DSS* stipulate very clear measures for data protection whenever cardholder data or sensitive authentication data is handled. The PCI DSS standard encompass all the system elements including networks, firewalls, servers, routers and other networking devices, applications, software code, databases, storage, scope of data stored, processes, access control, physical security, password management, cryptography, and more. Furthermore, it employs a rigorous certification process, monitoring and periodic reviews to ensure compliance while highlighting risks to help derive advance mitigation plans. Rezolve and the Rezolve platform maintains all stored, processed and transmitted cardholder and payment related data in line with the *Security built in*™ philosophy and in accordance with PCI DSS, including maintaining cardholder data in a secure wallet service which issues and uses tokens in communications with other system services, so obscuring and minimizing the potential attack surfaces to further mitigate risk.

**PCI DSS - The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.*

Payment Processing

For added security Rezolve does not process payments directly, but instead connects to and leverages the secure payment processing capabilities and networks of globally renown and certified payment providers. Rezolve orchestrates the commerce user experience and order and payment flows, connecting to payment providers' platforms through their existing secure APIs using authentication credentials provided and controlled by those parties. In this way Rezolve limits exposure to risk, and benefits from the leading security measures implemented and maintained by payment systems that are routinely and safely handling hundreds of millions of dollars' worth of payments transactions every year.

Protection of Personal Identifiable Information

Rezolve understands the importance of protecting personal identifiable Information (PII) and targets compliance with the rigorous General Data Protection Regulation (GDPR) standard due to come into effect in 2018. Although the GDPR is an EU initiative it is recognized as a strong standard with which many global organizations holding consumer data aim to comply. It not only addresses data protection within the EU, but also the export of personal data outside of the EU. Having an early sight in the GDPR ensures that Rezolve is implementing industry leading standards of PII protection.

Know Your Customer (KYC) and Anti-Money Laundering (AML)

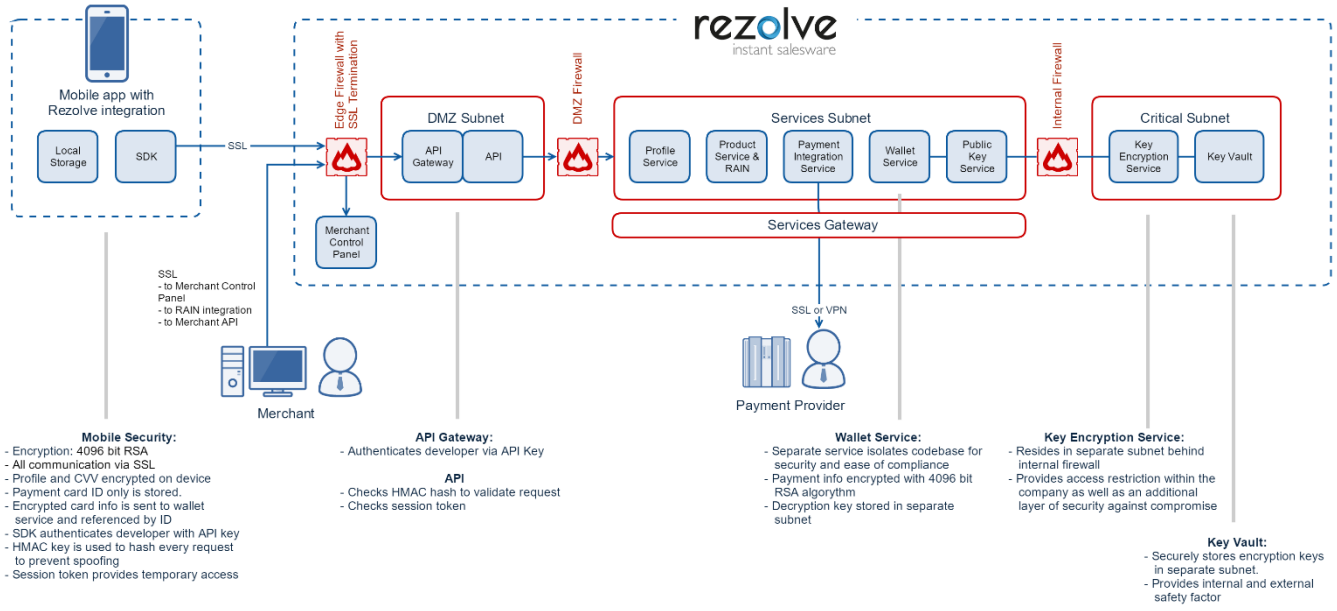
All organizations engaged in finance, banking, and payments operate in an increasingly onerous

Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance environment. Rezolve helps its customers in their KYC and AML initiatives through its in-built user behavioral data collection; Rezolve transactions build up a rich and comprehensive picture of users' identity, behaviors and preferences, allowing Rezolve's customers to ascribe higher levels of KYC and AML in relation to Rezolve transactions.

Data Sharing

Rezolve does not share data with any external agencies except as needed in the delivery of its service to its customers or where required by law.

Security Architecture Summary



Rezolve
https://www.rezolve.com/