DWOLLA

Security White Paper

Contents

Abstract

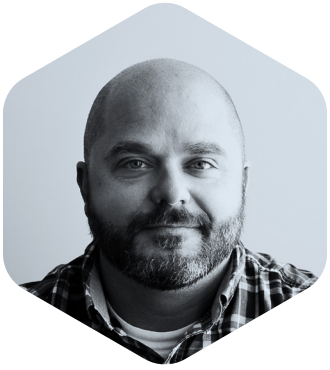
Security is a key piece of the Dwolla Platform. Our Information Security (InfoSec) team is proud of the practices they employ to protect our data from potential adversaries.

> ***Yet security work is never done.***

The more pride we take in our work, the harder those adversaries try to undermine our efforts. With this white paper we want to share how Dwolla does security and the thoughtful approach Dwolla takes with InfoSec.

Ben Schmitt, Dwolla's Vice President of Information Security, is a believer in using a defensive strategy against prospective threats.

As a member of SecDSM—a monthly meetup providing networking opportunities for InfoSec professionals—Schmitt says he's learned that simply being a "defender," without understanding who he is defending against, is only half the battle. That knowledge has affected many of his InfoSec philosophies.



"So now we are continuously testing because we should know some adversarial techniques. There are tools and techniques we can use against ourselves to validate that our controls are working. So my team's job isn't just to play elite defense, it's to know how the offense works too. For example, we monitor for lateral movement across systems and validate our alerting through the generation of inter-segment traffic attempts."

BEN SCHMITT, VICE PRESIDENT OF INFORMATION SECURITY

Dwolla's InfoSec team put together the following white paper to go into detail about the practices Dwolla uses to protect and store data. The white paper discusses cryptography, endpoint security, border protection and what we provide customers looking to integrate with Dwolla.

Introduction

Dwolla's mission is to build the ideal platform to move money. Securing our platform requires iterative security that evolves alongside our technology, people and culture. We focus on the protection of data and identities across our platform and our company. As a learning organization, we are never done with security; we seek newer technology, process, risk assessment and independent testing to continue to improve.

Dwolla has a dedicated and cross-functional security team charged with protecting the platform, data and identities. Our security team is responsible for the execution and management of our security program with a foundation in the CIS Critical Security Controls and the SSAE 18 SOC 2 Trust principles. The program is audited and assessed by third parties and customers.

The delivery of technology is driven by a secure software development life cycle grounded in careful design, code reviews, ruthless automation, continuous monitoring, automated testing/scanning and improvement. The Dwolla InfoSec team is seated within the Engineering area of our office to continually partner on design/architecture decisions, testing and implementation of new solutions. The partnership across Information Security and Engineering emphasizes using known secure defaults, architectural reviews, safe and standards-based cryptography across a platform powered and protected by AWS and Cloudflare technologies.

Training Across the Organization

All Dwolla employees are required to complete annual Information Security and Privacy training. This training is held for new employees joining the company as well as annually for all employees.

Dwolla uses a combination of current and customized topics to drive training, including:

- ✓ *Current threats and countermeasures (such as Spear Phishing)*
- ✓ *Emerging technologies*
- ✓ *Policies and procedures for the identification and reporting of security and privacy issues*

All Dwolla employees are required to use hardware-based (YubiKeys) multi-factor authentication for collaboration tools, password vaults, servers and remote access where possible. The Dwolla InfoSec and Engineering teams receive advanced Information Security training focused on the OWASP Top 10 risks, advances in modern standards-based cryptography as well as a case study focused on API and platform security research.

The Dwolla InfoSec team is dedicated to and focused on the protection and identities across the Dwolla Platform and the company.

Our security team reports directly to the CEO and is accountable for security compliance efforts (such as the SOC 2 Type 2 report), digital forensics and incident response, security operations, security design and data protection. Certain team members maintain current SANS GIAC certifications based on secure administration as well as incident response and forensics. To deliver security controls which match the needs of the Dwolla Platform, the security team uses a combination of commercial and internally developed solutions to aid in preventing, detecting and correcting security events.

Cryptography and Data Protection

Dwolla seeks to protect the confidentiality and integrity of data using NSA Suite-B aligned cryptography based on Authenticated Encryption and safe TLS configurations. We do this in three ways:

Data in Transit

The movement of data across trust boundaries requires a secure channel which authenticates and protects messages. Dwolla uses a configuration of TLS based on safe and current versions (≥ 1.2). Using a combination of techniques such as HTTP Strict Transport Security (HSTS), forward secrecy, secure renegotiation, downgrade attack prevention and cipher suite negotiation, Dwolla maintains an A+ rating from ssllabs.com. The Dwolla Platform does not permit non-TLS (plaintext) traffic.

Data at Rest

Storage of data at rest is achieved through the application of symmetric key encryption or cryptographic hashing. For the storage of data which must only be compared (such as a password), data is protected using a password-based hashing algorithm (pbkdf2) using appropriate work factors. Data which requires decryption is stored using the AES standard based on 256-bit keys and Galois Counter Mode (GCM) providing Authenticated Encryption with Associated Data (AEAD).

This method of encryption provides a combination of confidentiality, integrity and performance:

Key generation and cipher implementations are based on standards-based libraries (Java Cryptography Architecture Standard, Microsoft .NET System.Security.Cryptography), cryptographically secure pseudorandom number generators (CSPRNGs) and appropriate sources of kernel-mode entropy. Ongoing key rotation is achieved via automated generation and rekeying operations.

Tokenization

The Dwolla Platform is aligned with the OAuth 2.0 specification providing an API based on tokenization with two important features: replacement of high value data within transactional messaging and for an ongoing authorization model that refreshes tokens on a frequent basis. Dwolla tokenization decreases the value of financial transaction messages as sensitive information is replaced with a token and unique identifiers.

The user of tokens provides multiple layers of additive protection: reference, timing, scope and cryptography.

Reference

Dwolla does not share high value data such as a Bank Account or Routing Number for transactions with the other party.

Scope

Tokens have a collection of authorized actions in the form of a scope. The scope contains the range of actions that can be taken.

Timing

Dwolla requires that tokens have a expiration time frame of one hour. If a token expires, this access token must be refreshed.

Cryptography

Tokenization enlists cryptography to secure the information in transit and uses randomization to ensure each token is unique.

Endpoint Security

Devices owned and secured by Dwolla are required for access to Dwolla resources. Each Dwolla endpoint is monitored using known-good configurations, multiple security agents (malicious code/ suspicious network traffic, process and file monitoring) and continuous, credentialed vulnerability scanning and system updates.

Endpoints use encrypted filesystems, block mass storage devices and lock when idle. Remote access is controlled via authorized groups and the successful multi-factor authentication process which requires all of the following: userId/password, Dwolla-issued machine certificate and a hardware-based one-time password provided via YubiKey and Duo Security solutions.

Monitoring

The Dwolla Platform is monitored 24/7/365 using a combination of internal and external tools and services. Dwolla Platform API endpoints are continuously monitored using multiple third-party services. Infrastructure, service and event monitoring is based on centralized log collection, analysis and alerting. Engineering and Information Security teams follow escalation procedures to provide continuous coverage for the platform. Dwolla endpoint devices and internal infrastructure elements (wireless, firewall, IDS/IPS, servers, etc) additionally send logs off-site to a trusted third party for further analysis, correlation and alerting.

Border Protection

Dwolla uses a combination of AWS virtual private clouds (VPCs) and an Enterprise partnership with Cloudflare to provide a secure and highly available platform edge. The Cloudflare edge secures Dwolla's DNS entries and domain registration, enforces TLS negotiation for all connections, protects against volumetric distributed denial of service (DDoS) attacks and defends against abuse through the use of rate limiting and web application firewalling.

Vendor and Customer Review

Dwolla maintains detailed review processes for its vendors and customers that include Information Security components to manage third-party risk across the platform:

Vendor Review

Dwolla maintains a risk-based program to manage and protect sensitive information that is shared with external vendors. Adequate contractual language and due diligence processes support the protection of Dwolla Platform data. Dwolla maintains a Third Party Risk Management process to evaluate third-party vendors, collect assurance documentation, track issues and review progress on a go-forward basis.

Customer Review

Dwolla customers perform an Information Security review as a part of platform onboarding activities. The review includes an evaluation of authentication, authorization, application security, vulnerability management and data protection controls across the partner application.

Vulnerability Management and Independent Testing

Dwolla maintains ongoing vulnerability management activities across the platform using a combination of internal and external services and firms to identify and remediate risks:

Code Deployment

Each Dwolla merge requires a code review by an additional engineer prior to approval focusing on coding convention, unit/integration tests and security soundness. Subsequent to an authorized and approved merge, web deployments require a security scan by a third-party tool to identify, track and monitor potential vulnerabilities.

System Vulnerability Management

Systems are routinely scanned using a credentialed vulnerability scanning solution to detect potential configuration baseline deviations and vulnerable software which may require updating. Automated software update solutions are used to provide ongoing patching while immutable architecture is used to perform rolling deploys of load-balanced services for rapid software updates without downtime. Dwolla server instances are automatically updated upon deployment and authentication is MFA-controlled.

Independent Testing

Dwolla maintains relationships with multiple external providers of security assessment services. Dwolla performs penetration tests on a bi-annual basis covering external and internal environments. In addition to penetration testing services, Dwolla performs multiple audits focused on control review including the design, implementation and operating effectiveness of controls over a period of time. Dwolla maintains a SOC 2 type 2 report focused on the Security trust principle. Dwolla also actively maintains a private bug bounty program and responsible disclosure process.