plooto

Next Generation Payment Security

Overview

APRIL 2016

Contents

Introduction

Payment security has gotten a lot of attention lately. Many companies have become victims of financial and sensitive data breaches. Lack of IT spending, complex architecture, technology fragmentation as well as antiquated and legacy systems have left many companies vulnerable to cyberattacks.

This is precisely why Plooto's number one priority is security. Our cloud based solution delivers the most secure and most up to date security standard on par with many top financial institutions. Plooto consistently meets or exceeds the stringent security requirements of even the most security conscious organizations including Fortune 500 companies, the world's largest financial institutions, and other global companies.

The following overview was developed by Plooto in order to give our customers and users visibility onto our continued efforts to provide the highest level of security standards.

Overview

Plooto is a business payment management platform. Plooto has been designed from ground up with security, compliance and a wide set of security features in mind. This overview identifies security guidelines and processes we have put in place to ensure continuous delivery of a secure platform that surpasses customer expectations.

Plooto empowers businesses to send, receive and manage domestic and international payments using a cloud-based platform, all while maintaining an unprecedented security standard as part of its core development requirement.

In the following pages, we provide an overview of our security approach, which encompasses a number of key areas, including our security certifications & tests.

Payment Network

All Canadian payments processed through Plooto are settled through our partnership with members of the Canadian Payment Association (CPA). Plooto's payment technology is built on top of the existing banking infrastructure which is developed and maintained by CPA.

CPA is a non-profit organization that operates clearing and settlement systems in Canada and is responsible for the following:

- Operate and maintain national systems for the clearing and settlement of payments and other arrangements for making or exchanging of payments.
- Facilitates the interaction of the CPA's systems with others involved in the exchange, clearing and settlement of payments.
- Facilitates the development of new payment methods and technologies.

As a trusted CPA partner, we process our payments using the same technology as used by the big five banks. Plooto can process payments to any Bank or Credit Union in Canada and US. As part of our integration process with CPA, Plooto underwent verifications and approvals within the following key areas:

Full company background and risk analysis

Full financial and background auditing of our business processes and financials was preformed by our banking partners.

Secure data transfer/communication

Our system was validated for both incoming and outgoing data exchange using secure channels. Secure File Transfer Protocol is designed by Internet Engineering Task Force (IETF) and is powering data exchange for most major financial institutions.

System integration compatibility

Continuous tests are performed to ensure payment instructions are reflecting user actions during the payment cycle. We also run daily tests to ensure that the system is responsive for both recipient and sender's bank communications.

In conjunction with CPA requirements, we've implemented additional in-house security measures such as policy based fund clearing, bank account ownership verification as well as personal identity verification for advanced features.

Cloud Platform Infrastructure

All of Plooto's infrastructure elements are hosted by Microsoft Azure through its Infrastructure as a Service (IaaS) business unit.

Microsoft, with its unique experience and scale, delivers cloud services to many of the world's leading enterprises and government agencies. Today, the Microsoft cloud infrastructure supports over 1 billion customers across their enterprise and consumer services in 140 countries and supports 10 languages and 24 currencies.

Physical security

Azure provides geographically distributed datacenters that comply with industry standards (such as ISO 27001) for physical security and availability. Facilities are designed to run 24x7x365 and employ various measures from power failure to network outages. Centralized monitoring is administered by operations personnel.

Antivirus and antimalware

Virus and antimalware software scans all production and testing deployments using industry certified tools that ensure clean and stable environment. Routinely scheduled scans ensure that in the event of a breach systems will remain threat free.

Network and Data isolation

Logical isolation and segregated environments ensure confidential data remains inaccessible to unauthorized parties.

Encrypting data at rest and in transit

All traffic within our application is encrypted using built-in cryptographic technology using TDS (Tabular Data Stream) and SSL (secure sockets layer) when stored on Azure's data centers. This ensures that our data is never exposed to unauthorized third parties.

Plooto Platform

Plooto's secure platform encompasses our network and data security, platform security and workflow security.

Network/Data Security

- **End-to-End Encryption**
  All communication between users and Plooto is encrypted using the latest Secure Hash Algorithm 2 (SHA2) SSL Certificates. This standard is being utilized by top financial institutions and ensures no data is intercepted by unauthorized parties.

- **Encrypted Internal Communication**
  All internal system data remains encrypted (using SSL) to prevent loss.

- **Data Encryption**
  All customers' sensitive data is encrypted using AES 256 bit (Advanced Encryption Standard). This standard has been widely adopted by Canadian and U.S. governments and is utilized worldwide.

- **Data at Rest Encryption**
  Additional levels of encryption are applied to ensure data is encrypted while residing on physical hardware.

Platform Security

- **Staff Background Checks**
  Our support and security personnel go through a thorough background checks by Garda Inc.

- **Customer Data Access Monitoring**
  Access to the data by personnel is monitored, auditable, enforced by roles and is secured through multi-factor authentication.

- **Proactive Security Policy**
  Plooto enforces password policy with enough entropy to be next to impossible to break. Passwords are not stored in clear text but rather hashed using PBKDF2 (Password-Based Key Derivation Function 2). Failed authentication attempts are tracked. Additional attempts will trigger security verification and could cause the account to be locked in severe cases.

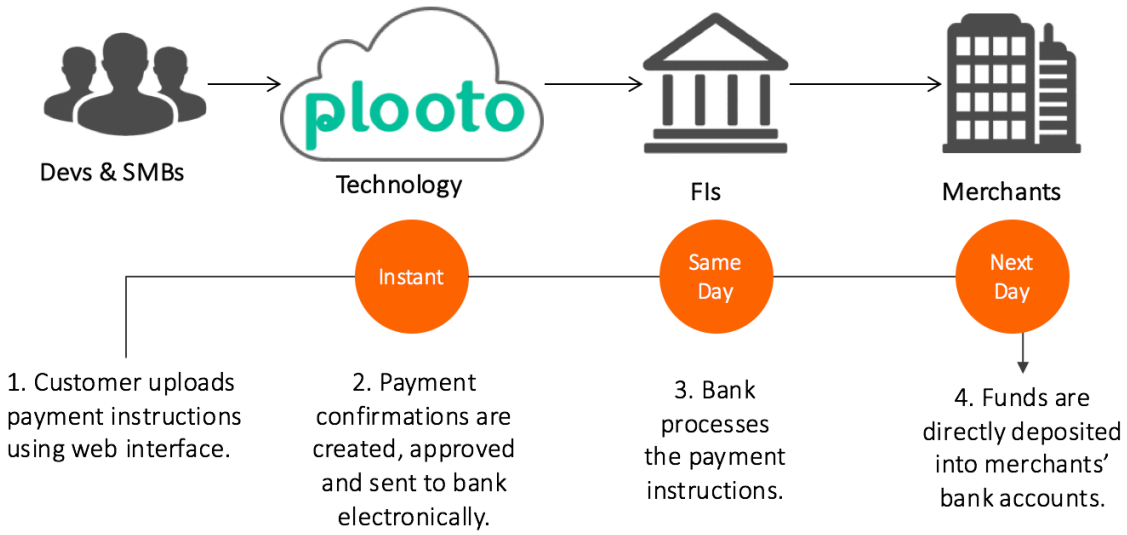
Workflow Security

Customers who want to mirror their existing workflow (multiple co-signers, accountants, compliance etc.) can either select one of our default permissions or create their own.

- Choose who initiates payments
- Choose who adds bank accounts
- Choose who adds payees
- Choose who approves payments
- Choose who customizes company information

How Plooto Works?

Plooto works with existing banking infrastructure to reduce friction and costs.



When a transaction is submitted, Plooto sends the instructions to the banks to have them transfer the funds between two accounts. Payment instructions are subject to sophisticated algorithms banks use in order to validate the information.

Bank Account Validation

Financial institutions use sophisticated mathematical algorithms to generate and authenticate account information keyed into their system. Transaction instructions submitted by Plooto to a bank are validated using these algorithms.

Modulus Check Digit Routines use checksum formulas in order to validate account numbers. The Modulus 10 routine is used by Plooto, financial institutions and government agencies as a method of distinguishing valid numbers from mistyped or otherwise incorrect numbers. These algorithms were specifically designed to protect against accidental errors when entering bank account information electronically.

Modulus routines involve multiplying some or all of the digits in the branch and/or account number by fixed numbers (the weighting factors). There is a specific weighting factor for each digit used in the verification process. The result of each multiplication is summed and the total divided by a specific modulus number.

In the event banking information is reported as invalid, the Plooto system flags the transaction and electronically notifies our system administrators.

Conclusion

Plooto's security approach is comprehensive. We meet or exceed national security standards and deliver exceptional financial and data security. Our continuous improvements and well as close partnership with leading technology and payment providers demonstrates our commitment to world-class security. We consider our customers' security priority number one. Our security approach encompasses everything from our people and processes to our platform and participants – senders, receiver, partners and developers. Our robust strategy allows us to ensure the confidentiality, integrity, authenticity, and nonrepudiation of our customers' payment information, and enables us to deliver 99.99% average uptime and availability of our system.

About Plooto

Plooto is a business payment management platform. Plooto automates and streamlines the way companies pay one another. Plooto was named one of CIX's top 20 most innovative companies in Canada.

For Inquiries: Local (416) 479-9656 | Toll-free 1 (844) 4PLOOTO (475-6686) | Plooto.co | @PlootoInc
Address: 111 Richmond Street West, 5th Floor, Toronto, ON, M5H 2G4