SeaCat and Point-of-Sale (POS) System Integration Manual

An architecture and integration guide to building and operating secure, scalable POS systems with SeaCat technology

The paper is intended for:

CISO, Point-of-Sale System Architects, System Integrators, and POS Operators

Table of Contents

Introduction

More and more businesses are adopting POS systems every day. This is because POS systems make it easy to track sales, manage inventory, take care of customers faster, and simplify the accounting process. In addition, they also allow businesses to gather marketing data, target the right customers, and offer them relevant promotions from the POS systems; thereby increasing customer engagement and boosting sales.

A POS system consists of a POS application that runs on a single-purpose hardware device. The system is usually connected 24/7 to a data network. The POS system is not a stand-alone solution usually; it integrates with other systems such as CRM, finance, warehousing, inventory management, or data backup to provide a more comprehensive POS system to the end-users.

There are four major challenges facing providers and operators of large-scale POS systems: Security, Reliability, Supportability, and Scalability. In following sections, we will elaborate on each of these challenges and how TeskaLabs' SeaCat technology can address them successfully.

Security

POS applications face a wide range of threats on a daily basis, from malware infection to unauthorized access, and even hackers taking direct control of POS devices. Hackers may exploit these systems to steal sensitive personal data such as credit or debit cards which they can then use to steal money from customers. SeaCat technology helps identify suspicious and fraudulent POS transactions, and protects customers' sensitive data by ensuring sales data only available to authorized personnel, preserve its integrity and accuracy.

Reliability

Retailers and businesses in hospitality, restaurant services, transportation and other industries need their POS applications to be reliable at all time. This is particularly important in fast-paced environments that require a consistently high level of customer services. Dysfunctional POS systems can affect sales, increase pressure on staff, and negatively affect the customer experience. SeaCat gives POS operators the necessary insights to quickly detect security incidents and ensures that POS systems are always available, so they don't have a negative impact on business operations.

Supportability

Companies that rely on POS systems don't expect any disruption to their business from cyberattacks or technical downtimes. They therefore need detailed insights into the usage, status, and connectivity of POS systems, to keep them running smoothly and prevent any wait time during payment processing.

SeaCat allows POS operators to support users of SeaCat-enabled POS system remotely, at any time. They have full access to the device, without needing to physically visit the location. This allows for 24/7 support, wherever the client might be.

Scalability

A scalable POS system saves time and money - especially when companies aim to expand their businesses in the future to many locations. SeaCat technology is specifically built for companies that operate and support large-scale POS systems. SeaCat allows businesses to scale and add more POS devices instantly, without impacting their existing workload. SeaCat gives POS operators the visibility and remote access capabilities they need to support systems running on hundreds, thousands or even millions devices across multiple locations, all without having to leave the office.

TeskaLabs SeaCat technology and O2 ’s point-of-sale eKasa

SeaCat

TeskaLabs’ SeaCat technology allows businesses to operate their POS applications safely and reliably and maintain full visibility of all POS applications and their activities. This guide will show you how SeaCat addresses the need for security, reliability, supportability and scalability when operating POS systems in heterogeneous network environments.

Reference project: O2’s eKasa

O2 eKasa is by far the most successful POS application on the Czech market. In 2016, the Czech government introduced a new regulatory requirement called EET (Electronic Evidence of Payment). This requirement meant that thousands of shops and restaurants now need to upgrade their technology and adopt a modern POS system. O2, the most successful POS seller during the first wave of November 2016 (more waves to come in following months), expected up to 150,00 concurrently connected POS clients daily. The eKasa system is secured by SeaCat to achieve desired visibility, availability, and data security.

Figure 1 - O2’s eKasa Point-of-Sale system

”It’s been a positive experience working with TeskaLabs. We needed to implement application security into our POS application very quickly, and we operate this service for our customers in a secure way thanks to TeskaLabs.”

Michal Ruda - Head of Business and Product Development, O2 IT Services

”Partnering with TeskaLabs was a very good decision for us. TeskaLabs' security solution makes things easy for both our project and application development teams. They can focus on delivery of the project and developing the application without being burden with the implementation of application security measures.”

Radek Žert - Project Manager, O2 IT Services

System architecture

SeaCat system architecture is made up of multiple components. The main ones are SeaCat SDK and SeaCat Gateway. SeaCat SDK is a library written in C, designed to integrate with the protected POS application. SeaCat Gateway acts as a shield for POS application backends. SeaCat Gateway allows only authorized data communication to reach the POS application backend. Between SeaCat SDK and SeaCat Gateway is a secure channel, which protects from many of the most common types of attacks, including Man in the Middle (MiTM). SeaCat Gateway creates an audit log for visibility, provides telemetry information, manages the POS application via SeaCat Admin Panel component, and processes remote access to the POS app.

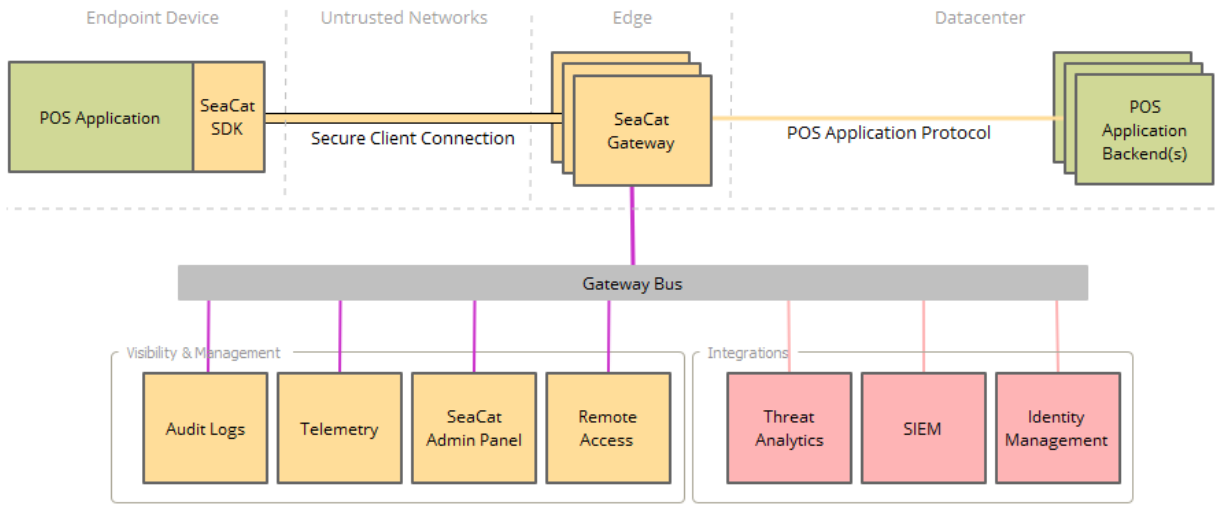

Figure 2 - Overall SeaCat architecture

Audit Logs

To react to security events immediately and properly, companies need to know that they are under attack. SeaCat technology provides companies detailed visibility into the data flow, activities of all POS applications, as well as actions generated from these apps. SeaCat Gateway' audit log contains an event description for every action performed at the SeaCat Gateway. The log also tracks other behaviors that affect the applications and the application backends such as availability, health status, and response time.

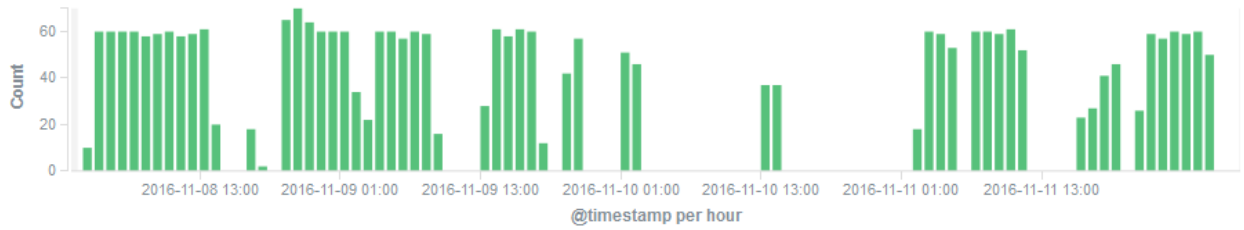

Figure 3 - Time-based graph showing client requests to a SeaCat-protected application backend

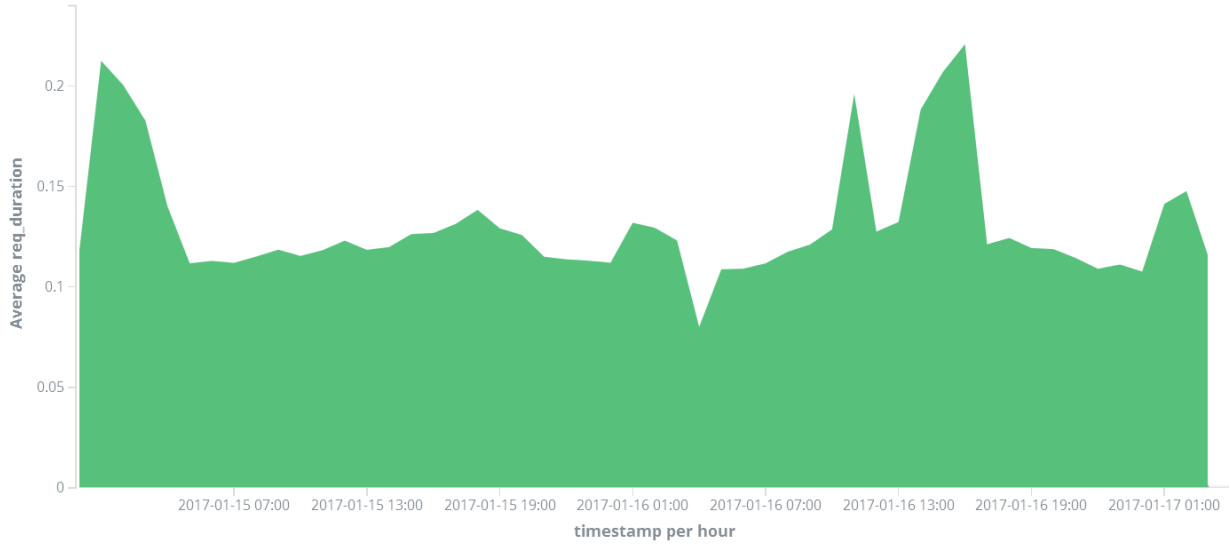

Figure 4 - Average time of responses from the application backend to user requests

Telemetry

Telemetry makes it possible to predict performance issues and optimize the hardware sizing based on the number of applications and their behaviors. Telemetry tool can also reveal anomalies in communications and trigger active response. It also provides information about SeaCat Gateway's current health status or performance and displays graphs that show hardware utilization.

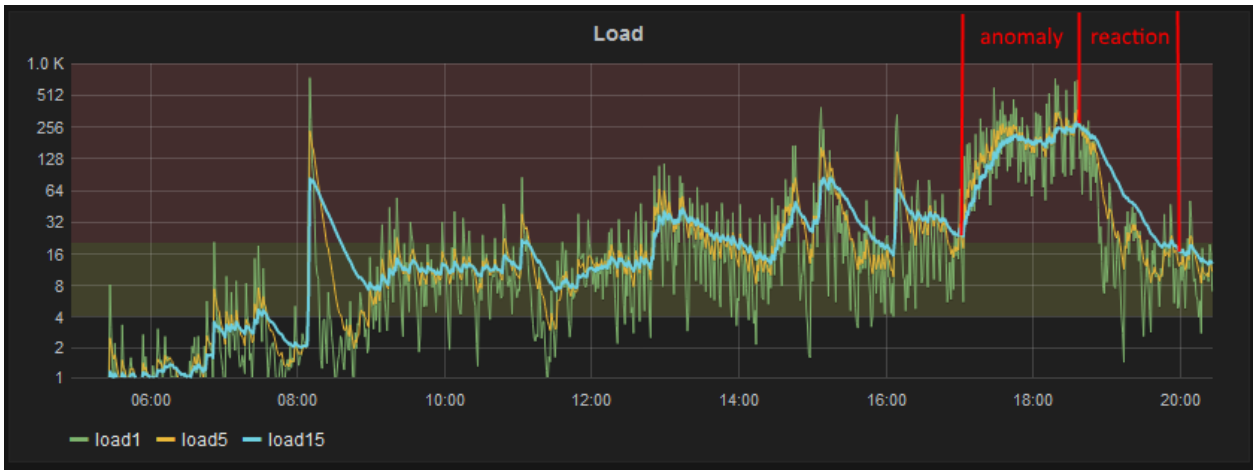

Figure 5 - Monitoring screen showing load anomaly to enable immediate reaction from operators

SeaCat Admin Panel

SeaCat Admin Panel functions as a built-in app management tool and offers detailed insights to all POS apps. The Admin Panel can be integrated with existing identity managements such as Active Directory to automate the management of users.

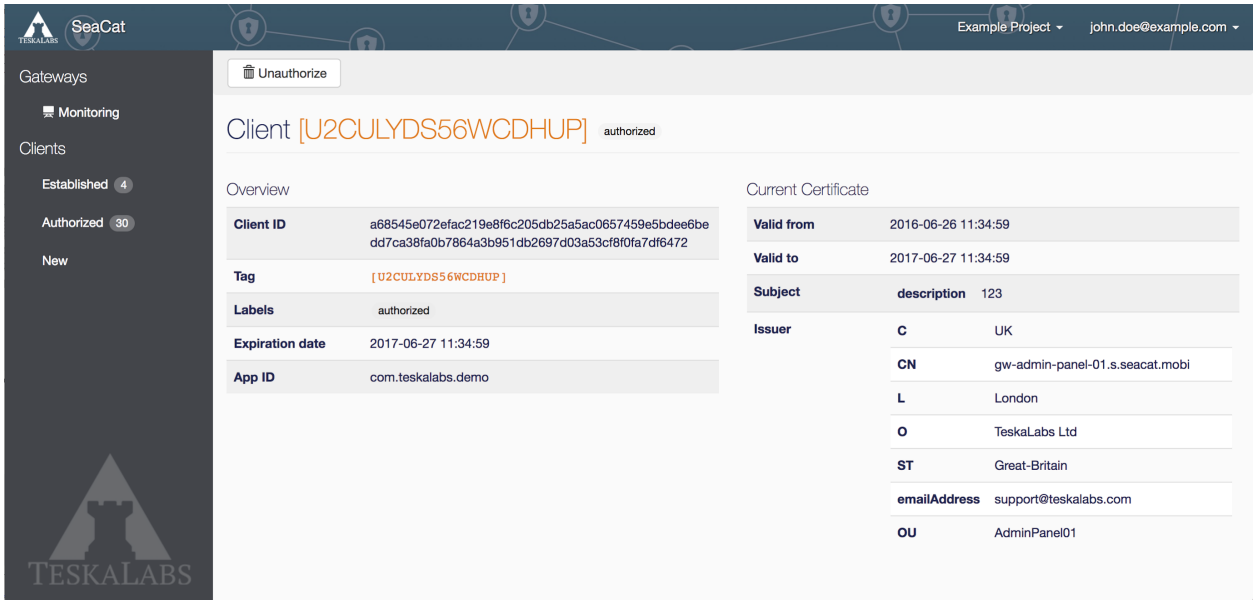

Figure 6 - Information of an application seen from SeaCat Admin Panel

Remote Access

Having remote access to POS apps allows POS operators to provide outstanding customer and tech support for their users, by quickly responding to and resolving issues. When POS operators respond to users in real time, help them use the app properly, and fix their issues, they increase user engagement and reduce the chance of users abandoning the app or switch to rival POS applications. Support and interaction with users is made effortless because operators can remotely access the POS app anytime as if they have the physical devices to hand, without spending extra time and money traveling to the site.

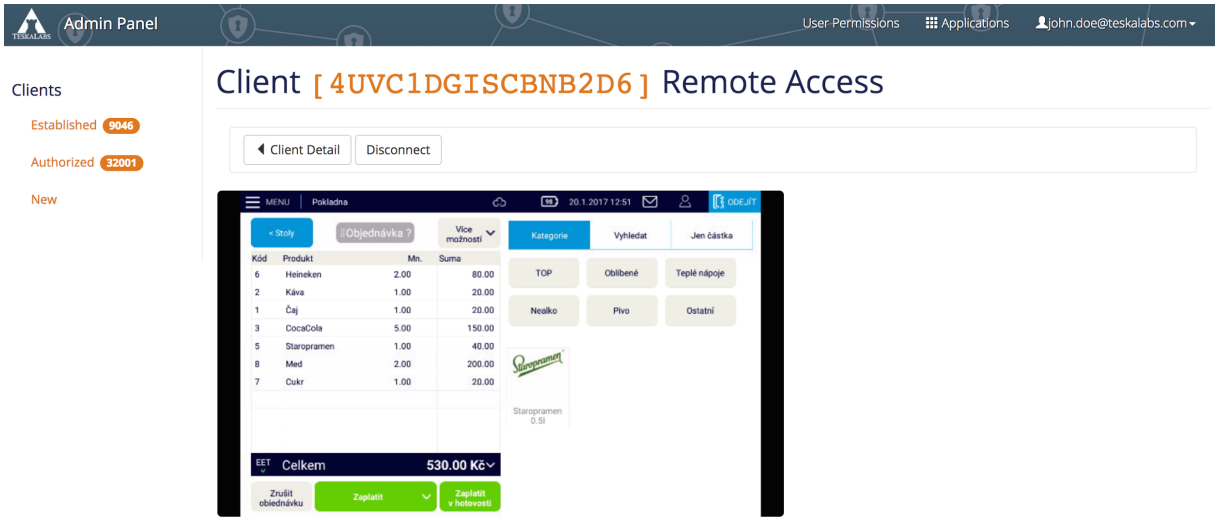

Figure 7 - Accessing the eKasa app remotely from SeaCat Admin Panel

Integrations

Integration with POS application

SeaCat has been specifically designed so that it can be easily added to new and existing POS applications. Integrating a POS application with SeaCat is done by putting the SeaCat SDK to the POS application through a few lines of code – this process only takes roughly one day to complete. SeaCat SDK is equipped with many bridges to allow integration with almost every mobile application platform, including Android, iOS, and even multi-platform frameworks like Xamarin and PhoneGap.

Communication between SeaCat SDK and SeaCat Gateway is transparent for the application. There is no need to change the functions of the POS application or the POS application backend API. The connection between the POS server and POS app is persistent, which reduces the consumption of data traffic as compared to a normal HTTPS connection. In comparison to HTTPS, the data connection handled by SeaCat is also persistent. Persistency of the connection allows access to the POS application from the server side, which makes POS update process or remote access from the customer support team possible.

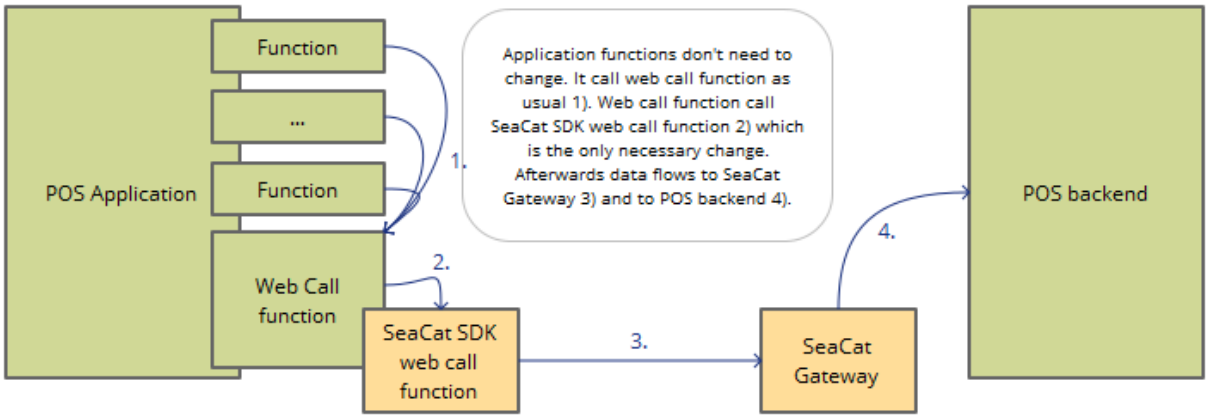

Figure 8 - Integration of SeaCat SDK

SeaCat technology is designed to ensure high availability of server-side services, thanks to no single point of failure architecture and load balancing ability. All POS application backends are entered in the SeaCat configuration, so that data traffic cannot be manipulated on the backend side. SeaCat Gateway deployment of the central SeaCat infrastructure usually lasts less than a week.

Integration to SIEM / Security Operation Center (SOC)

SIEM informs admins and operators about security incidents immediately, either during or before their occurrences. To predict and detect these incidents, it uses correlation rules and events sent from SeaCat Gateway to SIEM. Correlation rules are delivered as a part of SeaCat Gateway deployment. SIEM requires an audit log from SeaCat Gateway to identify these incidents. SeaCat Gateway provides this audit log via SYSLOG or CEF protocol.

Figure 9 – Example of SOC integration from O2 eKasa

Integration to Identity Management (IM)

All POS devices require user authentication. Often, these user credentials are stored locally on POS devices – an unsecure approach to user access management. Instead, SeaCat uses a centralized identity management for flexible and more secure user authentication. SeaCat can integrate with 3rd-party IM software such as Active Directory to automate the user management part. Furthermore, SeaCat Gateway pairs the POS user identification with the hardware device to significantly strengthens the security of user authentication.

SeaCat Gateway also supports LDAPS and other SSO technologies based on XML/SAML, to be as widely as applicable as possible. Alternatively, SeaCat provides its own IM function without relying on a centralized Identity Management.

About TeskaLabs

At TeskaLabs, we believe that the digital world has to be safe – and it's our duty to keep it that way. As enterprises move toward mobile and Internet of Things (IoT), we are here to help them build and operate mobile and IoT applications securely.

TeskaLabs is an award-winning product company committing to creating the world's most comprehensive application security technology for mobile and IoT apps. We are a proud member of Microsoft BizSpark Plus, a strategic partner of O2 Czech Republic, and a Cisco Solution Partner.

TeskaLabs operates from our headquarters in London, United Kingdom, with an additional office in Prague, Czech Republic. More information is available at www.teskalabs.com.

Contact us at info@teskalabs.com today to know more about building and operating your POS systems in a secure and reliable manner.