SALTEDGE

July 2018

Security, Privacy, and Performance

Table of Contents

1. Introduction

An ever-expanding number of leading FinTech companies, banks, and other financial institutions trust Salt Edge to deliver PSD2 compliance solutions, data aggregation API services, and white-label products. The trust is a result of the always-evolving information security management system, which includes policies, plans, audits, instructions and valuable documentation on “why” and “how” the information assets are being protected.

This paper aims to explain how Salt Edge ensures security and privacy of the data it collects, stores and/or processes, as well as how the company ensures security of its information systems in general.

In the context of financial technologies, the terms security, privacy, and trust are interrelated, but have different meanings. Security commonly refers to the confidentiality, availability, and integrity of data. Data security is the practice of keeping data protected from unauthorised modification, destruction, use and disclosure, by implementing physical security, software tools, and security policies.

2. Information Security and Privacy Governance

Salt Edge information security and privacy governance policy ensures that all the products are built in accordance with the company security and privacy restrictive terms and requirements.The products development phases are briefly explained below from a security and privacy point of view.

- **Design phase** – guiding security policies and required security trainings ensure that Salt Edge developers make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues at early development stages.

- **Development phase** – standard vulnerability types are addressed through the application of secure coding patterns. Also, static code analysis tools are used in order to identify security weaknesses.

- **Testing phase** – the company’s internal staff and independent security consultants conduct vulnerability assessments, along with manual security testing, in order to identify any potential security issues.

- **Production phase** – Salt Edge monitors the infrastructure in an automated way, and ensures that the developed functionality meets the company internal security requirements. Moreover, the company provides an incident reporting channel to its clients.

Salt Edge has a proactive approach toward information security. The company holds the ISO 27001 certification, which represents a guarantee of high security requirements and standards. A brief insight on how Salt Edge meets all the requirements related to main components of ISO 27001 certification:

- **Policies** – detailed internal privacy and security policies reflect how Salt Edge educates its employees about protecting the company's assets, and how the security measurements are carried out and enforced. The policies are being continuously adjusted to meet the most rigorous security requirements and standards.

- **Employees** – each Salt Edge employee receives regular information security and privacy trainings. Employees in data handling positions receive additional complex trainings specific to their roles.

- **Security staff** – the information security department, supervised by a highly professional CISO, is responsible for ensuring a military grade security within the company. Additionally, a certified internal auditor is in charge of conducting internal risk controls of the company's technology network.

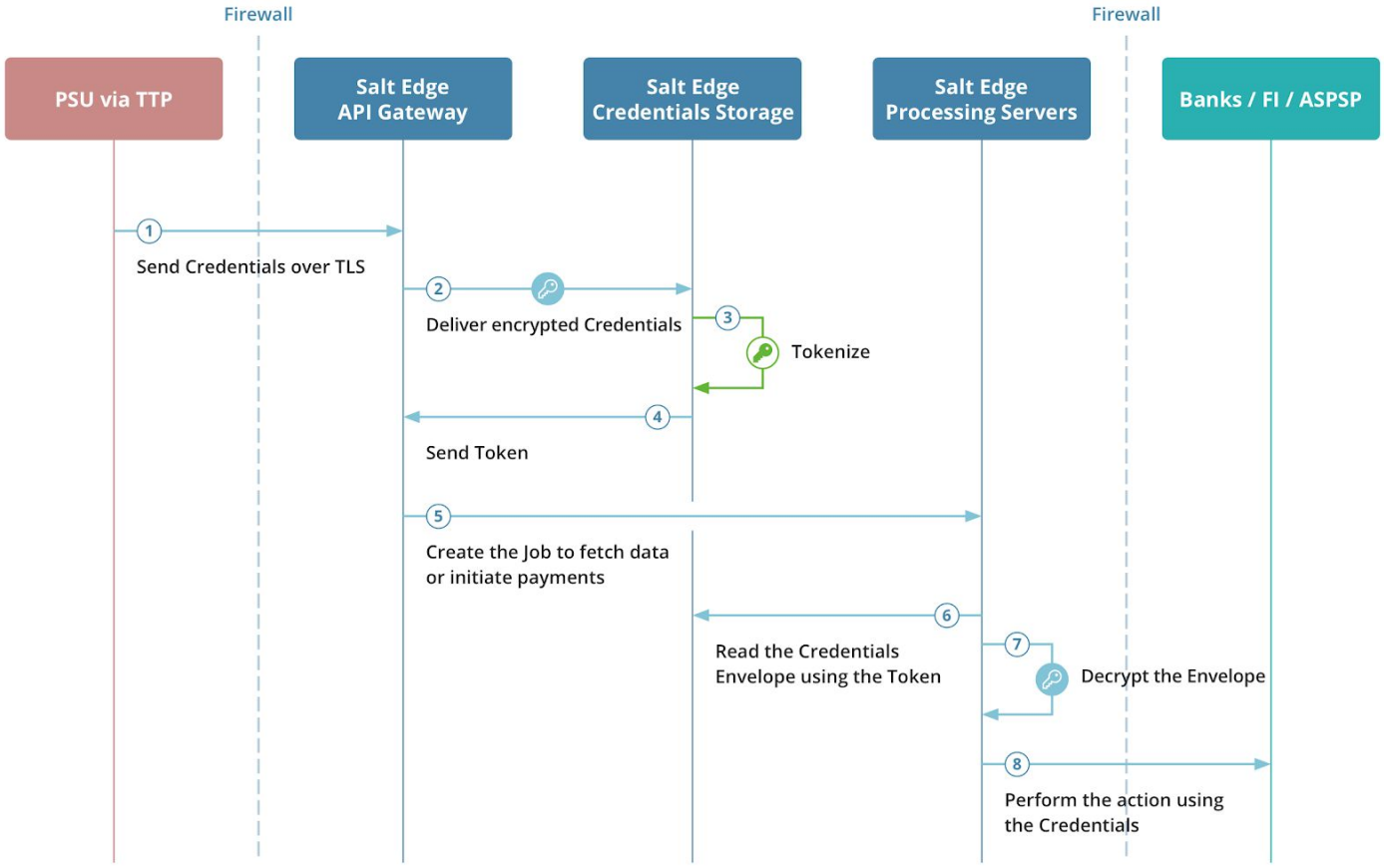
- **Assessments** – internal and external vulnerability assessments are regularly conducted, e.g., vulnerability assessments, security audits, and penetration tests performed by certified security service providers).

3. Infrastructure Security

The company staff continuously monitors the electrical, mechanical, operating equipments and software. Once an issue is detected, it is promptly addressed by qualified personnel. The maintenance is necessary for ensuring a stable and uninterrupted workflow of the company operations.

Access to the company systems requires multi-factor authentication. The databases are both physically and logically protected from general employee access. All employees sign a non-disclosure agreement before starting to operate. Once a new staff member is hired, he/she is only given access to the information required to do his/her job. All visitors are escorted by authorized personnel.

Salt Edge uses multiple defensive layers in order to protect end user data. Also, the company has implemented end-to-end encryption, an additional security layer to safeguard end-user credentials. Due to end-to-end encryption, the financial credentials are encrypted on end-user device or client backend before they reach Salt Edge infrastructure.



Steps:

1. End-customer shares Credentials with Salt Edge API Gateway via a secure TLS channel
2. Salt Edge API Gateway encrypts the Credentials with a public key, using RSA and AES 256 bit, and then sends them to the Credential Storage
3. Credentials Storage encrypts the credentials once more and creates a unique, one-time Token
4. Credential Storage sends the Token to the Salt Edge API Gateway
5. Salt Edge API Gateway starts fetching of the data or the payment initiation
6. Salt Edge Processing Servers read the encrypted Credentials using the Token
7. Salt Edge Processing Servers decrypt the Credentials using the private key
8. Salt Edge Processing Servers perform the action (fetch data or initiate payments) using the Credentials

Notes:

- All communication between parties is done via secure TLS channels
- Token - a randomly-generated string that can be used to access encrypted details only once

Salt Edge performs regular vulnerability scans to detect and classify the system weaknesses in computers, networks and communications equipment. This allows the company to predict the effectiveness of countermeasures. Eliminating any issue or system weakness that was detected during vulnerability scans, is a top priority for Salt Edge. Equipped with sophisticated encryption algorithms, the company products are compliant with PCI DSS requirements.

Salt Edge is regularly performing internal and external penetration tests in order to identify all the risks related to its network, services security, processes around the networks and applications. The gray box external penetration tests are conducted once per year by certified auditors. All the findings, if any, are addressed promptly and can no longer be replicated.

In order to ensure information system uptime, data integrity and availability, and business continuity, Salt Edge has implemented a Business Continuity/Disaster Recovery Plan. As part of the plan, Salt Edge stores all data in a ISO 27001 certified data center located in Germany. The encrypted backups are safely stored in a different data center.

4. Privacy in Salt Edge

Privacy most often concerns the digital collection, storage, and usage of personal data and information, including the transparency of such processes. In terms of financial technologies, the definition of **"Personal Information"** is any information related to an identified or identifiable natural person. Salt Edge employs advanced data protection and security techniques to safeguard user's personal information against identity theft and/or other related illicit access, use or disclosure. Salt Edge does not sell, lease or rent any of the personal information kept within its servers. When a processing system is secure and private, the company's clients develop trust in the provided services.

Salt Edge is committed to maintaining a high level of confidentiality, integrity, and security of any personal information. The company operates with three categories of information:

- **Public** - applies to information that is available on public resources.
- **Confidential** - applies to information that becomes available to Salt Edge and its authorized representatives pursuant to a signed NDA.
- **Protected** - applies to critical information (including personal data) that, if disclosed, could affect the company reputation, lead to legal investigations or even commercial penalties.

4.1 Privacy Principles

Salt Edge complies with the following common privacy principles:

- **Notice** – informing end users about the collection and usage of their personal information.
- **Consent** – asking for end user's permission to the collect and use of their personal information.

- **Access** – Providing End Users the ability to review, correct and destroy their personal information.

- **Security** – protecting personal information from various threats using industry-leading defensive barriers.

For more information on privacy policy, please access the Salt Edge website.

5. Reliability

Salt Edge uses a number of practices in order to ensure the reliability of its products:

- **Test recovery procedures** - Salt Edge regularly conducts tests on how the systems recover in case of malfunction. Such tests identify the problems that can be fixed prior a real failure scenario, and reduce the failing risk of components that have not been tested before. The test measures the recovery time in order to ensure that its duration does not affect the Service License Agreement.

- **Monitoring** - all the systems are being monitored for key performance indicators (KPIs), which can trigger notifications for DevOps team when a threshold is breached.[1]

- **Product architecture** - is designed to contain a set of microservices. This allows to scale and isolate the services depending on the volume and nature of processed data.

- **Multitenant data storage** - the users' personal data can be stored on multiple physical servers, which are isolated from each other. This allows the load distribution across multiple databases, and further improvement of security.

- **Horizontal scaling to increase system availability** - the products are designed to be served and processed by multiple small resources, in order to reduce the impact of a single failure on the overall system. The requests are distributed to ensure that they do not share a common point of failure.

- **Automated changes management** - the infrastructure changes are done in an automated, versioned, and reproducible way. This ensures that the environments are consistent across multiple servers, and reduces the resources provision time.

[1] For more details, please consult 7. Monitoring.

6. Logging

Salt Edge uses a distributed logging system based on ElasticSearch, which allows to perform a unified, scalable, and global audit of every action performed in the system.

- Logs do not contain any personal information or user credentials.
- Logs servers are isolated from application servers for reliability and security reasons.
- Access to logs is authorized.
- As any other system within Salt Edge infrastructure, the logs systems are being monitored as described in the monitoring section.

There are several kinds of logs that Salt Edge stores:

- System logs (Operating System)
- Network logs (Network hardware)
- Service logs (Database, Cache store, etc.)
- Application logs
- High level logs (interactions between multiple systems)

Additionally, Salt Edge uses a custom logging system for any interaction with external financial institutions. The access to these logs is permission-based and an expiration policy applies. The system allows to react to and fix the external errors as soon as possible.

The data stored in logs is used to debug problems, improve the customer experience and products performance[2].

7. Monitoring

The DevOps team is extensively monitoring company's systems and services to ensure that all the products have stellar availability and performance. The monitoring system operates with two main sources of data:

- Historical metrics from logs[3].
- Real-time system stats collected by metrics daemons, that are installed on each server (CPU usage, disk usage, process count, etc.).

All data is reported in real time to DevOps team on a visual dashboard. Important key metrics are defined based on this data. Each metric has an alert, which is configured to notify the DevOps team in case a predefined threshold is breached.

Besides the automated and data-driven tools for monitoring, Salt Edge has an incident reporting channel available to its clients, which they can use to notify Salt Edge for immediate action.

[2] For more details, please consult 8. Performance.
[3] The types of collected data are described in 6. Logging.

8. Performance

Salt Edge serves hundreds of thousands of end customers. Therefore, one of the company's top priorities is to ensure a consistent and fluid user experience. The company engineers take a data-driven approach to performance, by collecting a wide range of performance metrics from logs[4]. The performance enhancement is a never-ending process.

The process of improving the product performance has several logical steps:

1. Define the performance metrics;
2. Compare the current metrics to the previously defined ones, to determine the performance status;
3. Develop an action plan for the metrics improvement;
4. After the issue is fixed, perform a number of tests to confirm the successful fixing;
5. Monitor the metrics;
6. Repeat the process if necessary.

The combination of the performance alerts and the process described above, enable Salt Edge to ensure a 99th percentile http response time of 250ms for all its public endpoints.

From Salt Edge's experience, the performance is a systemic issue that can be improved on many levels. Usually adding a cache or a database index is enough, but there are also cases when going back to the drawing board and revisiting the core algorithm are necessary.

9. Legislative Compliance

9.1 General Data Protection Regulation (GDPR)

Salt Edge handles personal data of end users located worldwide, including individuals residing within EU. Therefore, the standards of data processing has to become compliant with GDPR by May 2018. This is the most impactful change in data privacy regulation for the past 20 years. GDPR is a regulation issued by the European Commission, the European Parliament, and the Council of Ministers of the European Union, with the goal to improve the protection of personal data within the European Union. Being compliant with GDPR means that the security and privacy of the provided services are always at the forefront of Salt Edge's business.

9.2 Revised Payment Services Directive (PSD2)

Salt Edge is part of the global financial technology industry. An important share of the company's clients are based and activate in the European Union. With January 13, 2018 the implementation date for the Second Payment Services Directive (PSD2), Salt Edge is preparing to become a registered AISP (Account Information Service Provider) and PISP (Payment Initiation Service Provider). Being compliant with AISP and PISP requirements under PSD2 means that Salt Edge has to maintain a high security and privacy level with respect to its services, servers, data centers, networks, employees, policies and business processes.

[4] For more details, please consult 6. Logging.

10. Conclusion

Assurance of data security and privacy builds the foundation of financial technology industry. Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of client trust and confidence.

Salt Edge offers its services to an ever-expanding number of financial institutions and their customers, all of which have entrusted one of their most important asset - the financial information - to Salt Edge. The company takes a complex and systematic approach to managing the overall information security and privacy aspects. Salt Edge has built an effective data security environment, where management from across the business departments works in a coordinated way and regularly assesses the effectiveness of the implemented policies. The systematic communication between company stakeholders ensures continuous improvement in raising and maintaining data security awareness.

Clients put their trust and confidence in Salt Edge, thus the company guarantees a high level of professionalism in safekeeping their privacy.

For additional details regarding Salt Edge's security, privacy and performance aspects, feel free to contact us.

About Salt Edge

Salt Edge specializes in intercommunication and interoperability between banks, Fintechs, and other financial institutions. Salt Edge is one of the most prominent bank connection networks, having 3100+ connected financial service providers in over 60+ countries worldwide.

That makes it possible for Salt Edge's clients to get instant access to, data enrichment of, and valuable insights into customer financial data. Such services include data aggregation, personal and business categorization, merchant identification, financial health check algorithms, KYC facilitation and much more.

For more information on Salt Edge products and services, please get in contact with sales@saltedge.com.