ORiON EDI Safety Documentation

OFFER VALIDITY:

25.05.2022

GRiT

Kopečná 10, 602 00 Brno, Czech Republic, T: +420 541 212 199, E: info@grit.eu, www.grit.eu
Business ID: 46963740, Tax ID: CZ46963740

Restrictions Regarding the Publication and Disclosure of Data

This document contains confidential information. It is intended exclusively for the clients of GRiT, s.r.o., to whom it was provided. As such, it may not be copied, published or provided to other natural persons or legal entities without the prior written consent of GRiT, s.r.o.

Table of Contents

1. Introduction

This document contains technical and functional specifications of the ORiON service, as well as data security-related organizational and procedural measures.

2. Service Description

The ORiON B2B/EDI solution a proprietary product of GRiT. The ORiON solution is designed as a platform, and, at the same time, as a service intended for electronic trading between entities communicating in agreed structured formats through various technical channels. It is offered to customers as a comprehensive service for EDI communication solutions.

2.1.1. Its key features include:

- **Message translation** – the solution translates messages between various formats (generally any fixed width type structured formats (flat file inhouses, etc.), delimited file formats (CSV, PDK, etc.) and XML-based files). The standard message data description is based on EANCOM definitions (a subset of UN/EDIFACT).
- During the translation, **unification of messages** of individual entities according to the available message type standard is used internally, which transforms the messages to a readable format suitable, for example, for use with a web interface or for emailing or faxing of messages in a readable format (HTML, PDF, etc.). At the same time, it greatly simplifies the process of new entities joining the communication without affecting any other entities.
- **Communication interface** – the system can be extended to include a communication interface so it can be easily used not just for automatic and secure communication between entities at the https level, but also for adding other communication channels, such as automatic communication in VAN networks, AS2, emailing of messages in data and readable formats, distribution of messages via ISDS solutions, faxing of messages, SFTP, etc.
- **Solution flexibility** – The solution is based on Amazon Web Services (AWS) cloud services and reflects the latest e-commerce needs. At the same time, it also supports the "traditional" EDI standards – EDIFACT.
- **Extensibility of the solution** – the architecture allows for the use of add-on modules and thus customer expansion, e.g. to include a catalogue of goods and prices, B2B e-commerce, etc.

3. Architecture

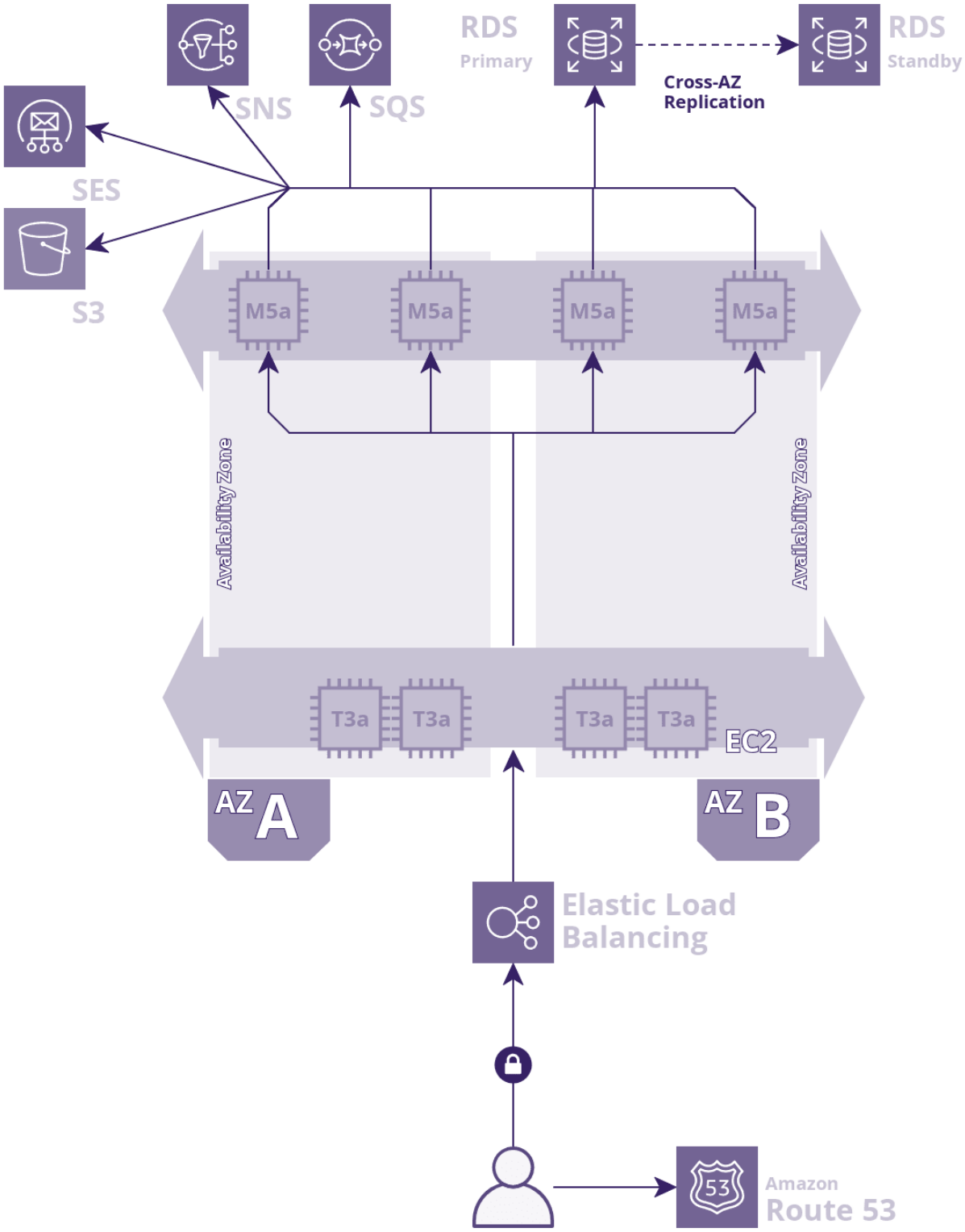
3.1. HW Platform Description

The key elements of ORiON run in the AWS cloud, where all the elements are redundant to ensure high availability of the solution.

3.1.1. Environment Specifications

- The solution was developed and runs in the AWS cloud
- To run the solution, AWS uses the following services: RDS, EC2, SQS, SNS, SES, Cloudwatch
- The database layer runs in High Availiability mode using MultiAZ deployment with a dislocated standby database
- The key elements of the ORiON solution are redundant (database servers, disk arrays, application servers), and thus remain operational even in the event of failure of any of these elements (e.g. failure of one array, one database server, etc.).
- In case of disaster recovery (e.g. a natural disaster), the solution uses multi-location backup with multiple locations throughout the EU.

3.1.2. Platform Infrastructure



3.2. Amazon Web Services Specification

Amazon Web Services (also known as AWS Cloud) is the world's most popular cloud computing platform for provision of online services offered by the U.S. company Amazon.com Inc.

The AWS Cloud infrastructure is built using AWS regions and availability zones. The AWS region is a physical location around the world, with several availability zones. Availability zones consist of one or multiple physically separate data centers, each of which has redundant power, networks and connectivity, and is housed in a separate facility. These availability zones offer the ability to run production applications and databases that are highly available, more fault-tolerant and more scalable than would be possible with just a single data center. AWS Cloud operates in more than 84 availability zones across 26 geographical regions around the world.

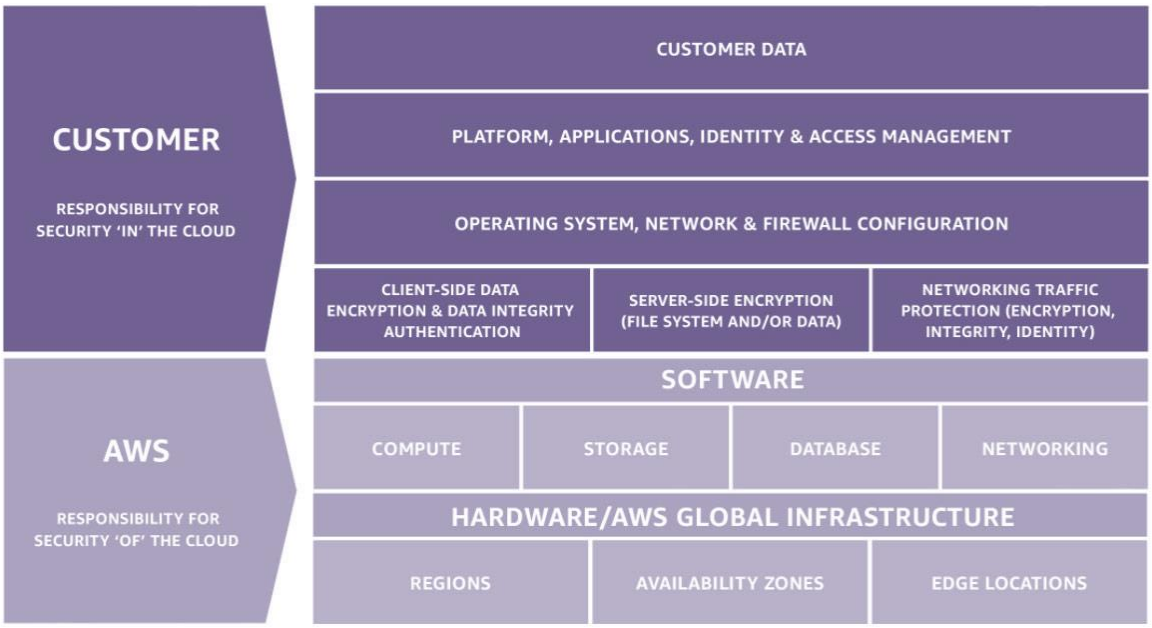
Each AWS region is designed to be completely isolated from the other AWS regions. This allows for the greatest possible fault tolerance and stability. Each availability zone is isolated, but availability zones within one region are interconnected by low-latency links. AWS provides the flexibility to place instances and store data across multiple geographic regions as well as across multiple availability zones in each AWS region. In case of failure, each availability zone is designed as an independent zone. This means that availability zones are physically separated within a typical metropolitan region and are located in areas with low risk of flooding (the specific categorization of flood zones varies by AWS region). In addition to discrete uninterruptible power supplies (UPS) and on-site backup production facilities, the data centers located in different availability zones have been designed to be powered by independent power distribution points to reduce the risk of an event on the power grid affecting more than one availability zone. All availability zones have redundant connections to multiple Tier-1 providers.

3.2.1. Security

Cloud security is similar to security in on-premises data centers - only without the cost of equipment and hardware maintenance. Physical servers and storage devices do not need to be managed in the cloud. Instead, software security tools are used to monitor and protect the flow of information to and from the cloud resources.

Another advantage of AWS Cloud is that it allows you to scale and innovate while maintaining a secure environment, while you only pay for the services you actually use. This means that you can have the necessary level of security at a lower cost compared to a local environment.

AWS Cloud enables a shared responsibility model. While AWS administers cloud security, GRiT is responsible for security in the cloud. This means that GRiT retains control over security, just like when using on-premises data centers.



AWS offers specific security tools and features with regard to network security, configuration management, access control and data encryption.

And, last but not least, the AWS environments are continuously audited, thanks to certifications from accreditation bodies across geographical areas and verticals.

AWS Certification:

- ISO/IEC 27001:2013
- SOC 1/2/3
- PCI DSS Level 1
- FIPS 140-2
- and others

3.3. Software/Application Architecture

The solution is physically located in the AWS data center in Frankfurt (primary site) and Ireland (secondary/backup site).

A three-tier architecture is used:

- Presentation layer – HTML + JS in browser
- Application layer – running on application servers in JAVA + Spring Boot framework
- Data Tier – Oracle Database as an AWS RDS service

In addition, the MVC and MVP design patterns are used.

3.3.1. SaaS

The ORiON application has been designed and is operated as SaaS (Software as a Service) and takes advantage of the Multitenancy principle.

3.4. Server Architecture Security

Service access to the architecture is possible exclusively via the secure SSH protocol in combination with a very strong password, certificate, and source IP restrictions (SSH + password + IP addresses).

Only authorized employees have access to the platform.

4. User, Role, and Permission Management

4.1. User Authentication

Enterprise Single Sign-On is used for user authentication. Enterprise SSO is based on Jasig CAS (for more information, visit https://apereo.github.io/cas/6.5.x/index.html)

The application does not support unencrypted access (only HTTPS access is supported). The username and password are thus never transferred in unencrypted form, but always through an encrypted channel.

4.1.1. Multi-factor Authentication

ORiON access can be limited for an organization to selected IP addresses so that access from other IP addresses is blocked. The administrator is always notified when a user tries to access the system from an unauthorized IP address.

Alternatively, the application can be set up to allow access from other IP addresses, but the administrator is always notified of this.

4.2. User Authorization

To grant permissions to individual users, a system of roles is used (the so-called RBAC – Role-based access control, for more information visit: http://en.wikipedia.org/wiki/Role-based_access_control).

Because of this, you cannot assign specific permissions to a user, only to a role or multiple roles. The roles are then assigned specific rights to access data, perform selected operations, etc.

4.2.1. Special Restrictions

The application also distinguishes 3 special types of users, to whom special restrictions apply:

- System Administrator – only employees of the operator can be assigned this role, multi-factor user authentication must be used by all system administrators.
- Organization User Administrator – the only role allowed to manage users and permissions within the organization
- Other users – standard users within the organization

4.3. Password and User Account Policy

The ORiON solution allows you to set various password policies (a stronger password is typically required for the administrator than for the user) for different types of users (user administrator vs. user).

Currently, the following password properties can be set for individual policies within an organization:

- the minimum password length
- the minimum number of digits
- the minimum number of uppercase letters
- the minimum number of lowercase letters
- the minimum number of special characters
- the minimum number of alphabetic characters

User passwords are not stored anywhere, the application works with encrypted password hash.

Other parameters that can be applied to password policies force periodic password changes and restrict the reuse of the same password:

- the minimum number of non-recurring passwords
- the maximum password validity period in days

4.4. Recovery (reset) of a forgotten password

To recover a forgotten password, the user will be sent an email with a unique link to the password change form, where the user can change the password.

The email is always sent only to the email address stored within the user account in ORiON. The sent link is only valid for a limited period of time.

The user can request the password recovery email him-/herself, from the login form, after entering his/her login name (they must know the login name). Password recovery is not available if the user account is locked or the user is disabled.

The email can also be sent by the Organization Administrator or the System Administrator from the ORiON user management.

4.5. User Account Locking

This is related to the password policy. User accounts are locked automatically if the organization set up a password policy in ORiON with a limited password validity period.

The user is notified of the necessity to change the password 14 days before the expiration of the password when logging in to the application.

The password expiration date is calculated from the date of the last password change. After the password has expired, the user's account is locked and can only be unlocked by resetting the password, which can only be done by the Organization Administrator or the System Administrator.

If the user account is locked, the user will be unable to reset the password using the login form.

5. Event Logging and History (Auditing)

The application uses two types of event logging:

1. Oracle DB-level logging (access to key entities, assignment and change of permissions, etc.)
2. Application level logging (batch processes, data processing, automatic operations, etc.)

When it comes to user actions, events are shown with the corresponding entities (e.g. document editing is shown with the given document, etc.)

5.1. Notifications

Beyond user based logs, there is also a general add-on called Notifications. For selected types of events it is possible to set up event notifications for users, who are then receiving email notifications to their inboxes.

The Organization Administrator can also be notified of events triggered by other users of the organization.

6. Processes and Standards

6.1. Development

For the maintenance and development of the ORiON SaaS service, we use the agile Scrum methodology.

For the recording and maintenance of requests throughout the organization, including development, testing and implementation (service), we use the Atlassian Jira ticketing system (https://www.atlassian.com/software/jira).

For software development we also use the Continuous delivery (CD) methodology, in particular in the areas of Continuous Integration and Continuous Deployment.

For CD we use the Teamcity tool (https://www.jetbrains.com/teamcity/). Gradle or Maven are used for build automation.

6.2. Testing

When developing solutions, we use several types of testing:

- unit testing (JUnit)
- integration testing (DBUnit, Selenium)
- acceptance and regression testing (tester)

In addition, within Scrum, code review is carried out by the senior developer and acceptance of functionality by the client.

6.3. Installation of Versions

Version builds are created using continuous deployment. The installation of the versions is then manual with scheduled system or subsystem downtime.

6.3.1. Versioning

We use GIT and the GitFlow workflow schema (https://www.atlassian.com/git/tutorials/comparing-workflows/gitflow-workflow).

6.4. Development and Test Environment

Using the above techniques and tools, software changes are published in a controlled manner from a separate development environment to a test environment. The tested and accepted version is then installed in the production environment.

7. Security Testing

The application architecture is built to allow automatic testing of code for artifacts, ensuring data security (typically the Multitenancy principle). If the condition is not met, the application build cannot be created.

7.1. Penetration Tests

For solution security testing, comprehensive **Qualys Scan** (commercial version) tests are run on monthly basis in the production platform.

8. Encryption and Electronic Signature

The solution uses cryptographic methods on multiple levels:

- For secure communication between clients (users) and the ORiON solution
- To store selected sensitive information in a database
- To ensure the authenticity and integrity of electronic documents
- For trusted archiving (anchoring of documents in time) to ensure long-term trustworthiness of electronic signatures

8.1. Communication Protocols

Only secure protocols are used for application access:

- https – only Transport Layer Security (TLS) is allowed here
    - currently TLS 1.1 and 1.2 is used
    - SSL is disabled because of the potential risk of POODLE attacks
- ssh (Secure Shell) – for service purposes only
- scp (Secure Copy) – for service purposes only

The application does not natively support insecure protocols.

For user communication with ORiON, transfers of user data to ORiON, etc., HTTPS communication is used exclusively.

HTTP access is prohibited.

8.2. Trustworthiness of the ORiON Application

To ensure maximum trustworthiness of user access to the ORiON solution, we use an EV (Extended Validation) SSL certificate from GeoTrust.

8.3. Electronic Signature and Document Encryption

Electronic signature and document encryption supports:

- Electronic signature as recommended by GS1 International for signing EANCOM messages
- EANCOM message encryption (CIPHER message)
- Electronic signature of PDF messages
- XML electronic signature as recommended by the ICT Union for ISDOC messages

For more information regarding the electronic signature, its verification and archiving of tax documents, see ***Paperless invoicing and archiving of invoices in ORiON EDI***.

9. Monitoring

9.1. Server-level Monitoring

The solution uses permanent monitoring of platform elements (servers, etc.), monitoring of their availability, and key OS parameters (disk space, processor load, etc.) using AWS CloudWatch.

9.2. Application-level Monitoring

Integrated monitoring tools are used for the application itself which monitor specific metrics (message and package queues, data processing rate, etc.).

10. Reporting

Upon request, automatic or one-off reports are available, which include information about user access to the application, new password requests, etc. The following are the most common reports:

1. List of new users in the organization
2. List of forgotten password requests
3. Information about failed log-ins
4. List of locked accounts
5. Report of user access from invalid IP addresses

CONTACT ORiON

Kopečná 10, 602 00 Brno

T: +420 541 212 199

E: info@grit.eu

www.grit.eu