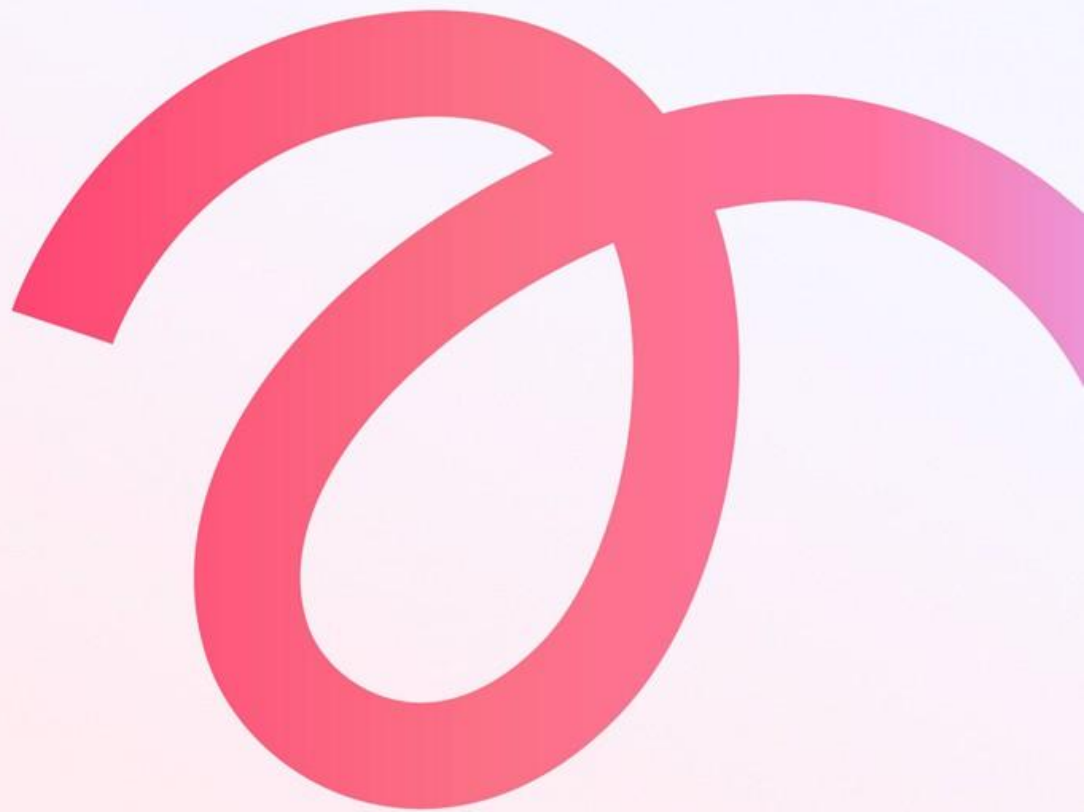


Security description

System platform

Confidential

Updated 30.9.2025



Contents

1	Introduction.....	2
1.1	About System.....	2
1.2	About the System cloud platform	2
2	Architecture	3
2.1	Network architecture	3
2.2	Common integration strategy with third-party components.....	4
3	Data centers.....	6
3.1	Data residency	6
3.2	Data removal	6
4	Data security.....	7
4.1	Data at rest.....	7
4.2	Data in transit.....	7
4.3	Data region and location	8
4.4	Ports.....	8
4.5	Domains and required network access	8
4.5.1	Required network access for System Visit kiosk devices	8
4.5.2	Required network access for System Rooms devices	10
4.6	Uptime and reliability.....	10
5	Application.....	11
5.1	Authentication	11
5.2	Development process.....	11
5.3	Audit trail and logs.....	11
6	Employee access, confidentiality, and data security	12
7	Use of sub-processors in service delivery.....	13
8	System platform	14
9	Appendix	15
9.1	List of abbreviations	15
9.2	General info and guidelines	15
9.3	Google security whitepapers	15

1 Introduction

This documentation, notation regarding paths, and syntax in figures and diagrams are used according to the architecture diagram. Here, you'll take a brief look at some of the commonly used features and get pointers on how Systemam has built its core services.

Systemam's infrastructure is built on the Google Cloud security foundations blueprint to identify core security decisions that'll guide us with opinionated best practices for deploying a secure GC environmentⁱ. Google Cloud Platform provides hyper-scalable cloud products such as Cloud DNS, Cloud Load Balancer, Cloud Run, Cloud Storage, Cloud SQL, and many more.

1.1 About Systemam

Systemam Oy is a Finnish software company, founded in 2006. We are experts in digital visitor management and better meetings. Our solutions automate routines, streamline meeting preparation, and reduce unnecessary fuss to ensure every meeting is safe, smooth, and productive – all with a single click. Our goal is to create safe and seamless workplaces where meetings count. We want to preserve the unique value of in-person meetings and see businesses thrive with safe and meaningful interactions, powered by data and connectivity.

1.2 About the Systemam cloud platform

Systemam cloud platform is the base for the service solutions that we offer, such as digital visitor management (Systemam Visit), safety inductions (Systemam Pass), meeting room displays, and room booking (Systemam Rooms). The platform is:

- Accessed through the web, mobile, and by using dedicated devices such as self-service kiosks (Systemam Visit and Pass) and meeting room displays (Systemam Rooms).
- Built and developed following the Google Cloud security foundations blueprint to identify core security decisions.

2 Architecture

Our services are built on top of Google's hyperscale data centers and infrastructure platform, Google Cloud Platform. We use multiple highly available and secure managed services, including but not limited to:

Cloud DNS	High-performance, resilient, global service that we use in both public and private zones. No customer data is transferred or stored in DNS.
Cloud Load Balancer	Fully distributed user traffic across multiple instances and services.
Cloud Run	A managed serverless compute platform to run containerized services with autoscaling behavior to scale to the number of instances needed.
Cloud Storage	Distributed object storage to store immutable data such as profile pictures or other static files.
Cloud SQL	Fully managed relational database that stores data that is encrypted at rest and in transit.
Pub/Sub	A synchronous and scalable messaging service for service integration.
Cloud Scheduler	Scheduling units of work to be executed at defined times or regular intervals.
Cloud Run Functions	Bound to events to implement asynchronous workloads, cloud automation and internal endpoints.

Table 1. Google Cloud managed services

All the above products and services are served from Hamina, Finland, except for Cloud DNS, which is a global service and does not contain any customer data.

2.1 Network architecture

The base representation of network architecture consists of multiple managed products and services that were disclosed in section 2. Communication between these components is within the disclosed region and encrypted and served through TLS.

Data is encrypted at every step of the way:

- From client to Cloud Load Balancer
- Cloud Load Balancer to Cloud Run
- Cloud Run to Cloud SQL
- Cloud Run to Cloud Storage
- Response back to the client

The following diagram will give you an overview of our service architecture and is a brief overview of service relations.

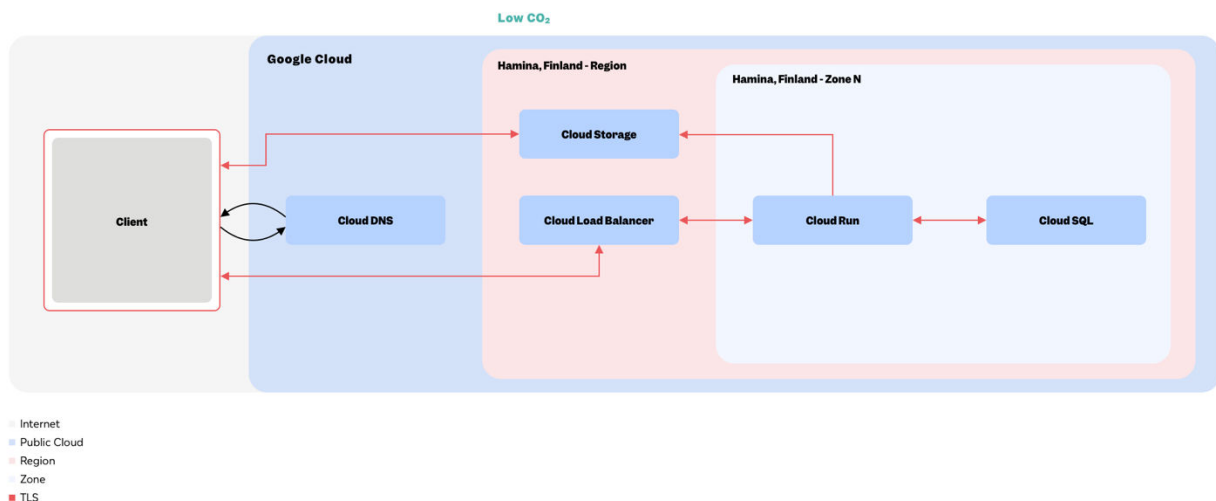


Figure 1. System service architecture

2.2 Common integration strategy with third-party components

Communication from the client to our platform, shown in section 2.1, to a third-party integration vendor is usually done via TLS, and certificates are verified by a third party on both ends. The following diagram will give you a visual representation of service architecture and the external entities involved.

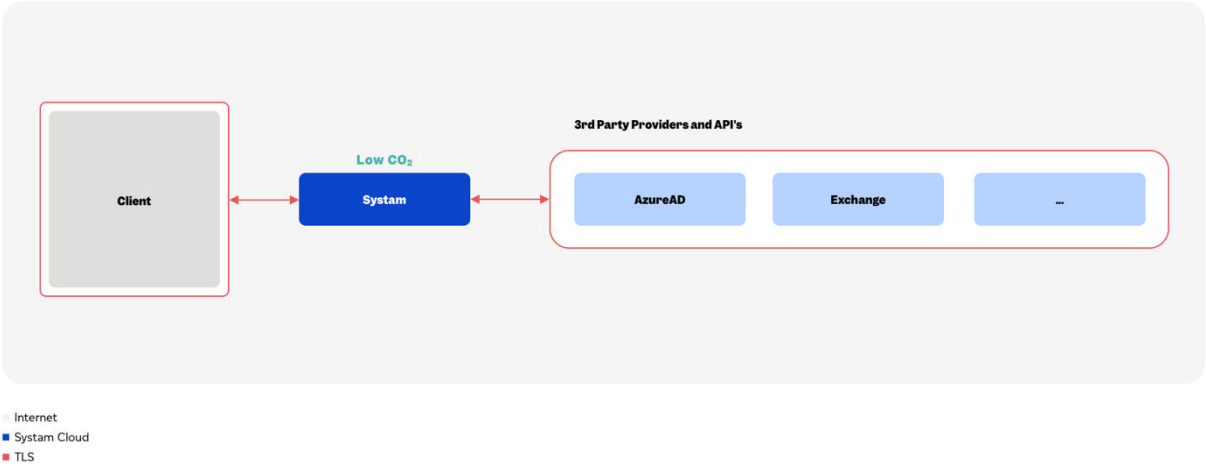


Figure 2. Integration to 3rd party software

3 Data centers

System is a cloud service and is hosted by data centers with the highest level of certifications and compliance, including ISO 27001, SOC2, GDPR, PCI DSS, PiTuKriⁱⁱ. For more compliance information, you can visit Google Cloud Compliance offeringsⁱⁱⁱ.

3.1 Data residency

All application servers and services are based in Hamina, Finland, but can be accessed internationally via the internet. Data is not replicated outside the Hamina, Finland region, as explained in section 4.3.

3.2 Data removal

All customer data is stored on Google Cloud services, which follow a strict decommissioning policy^{iv}. Customers own the data stored in their service and may at any time retrieve the information collected from the service. In the event of canceling the subscription or terminating the system, all customer information, applications, and settings from the server and backups are removed.

4 Data security

This section will go into detail about how System manages data and security across all boundaries. In general, encryption is done by using industry-standard techniques, which are disclosed in sections 4.1 and 4.2. Encryption measures are implemented to ensure the confidentiality and integrity of the data across the service.

4.1 Data at rest

Encryption at rest is a type of encryption that is used to help protect data that is stored on a disk. All data that is stored by Google is encrypted at the storage layer using the Advanced Encryption Standard (AES) algorithm, AES-256. Google uses a common cryptographic library, Tink, which includes our FIPS 140-2 validated module (named BoringCrypto) to implement encryption consistently across Google Cloud^{vi}

System manages the keys used in default encryption at rest using Google's Customer-managed encryption keys (CMEK). Cloud Key Management Service lets us create encryption keys that we can use to add envelope encryption to our data. Using Cloud KMS, we can create, rotate, track, and delete keys, and the system logs all access automatically. Additionally, user passwords are both hashed and salted using one-way encryption. Application credentials are stored separately from the code base using the Secret Manager. Clients authenticate using a token-based system. Each token has specific access scopes, which can be individually revoked without impacting other clients.

- Uses Google's Customer-managed encryption keys (CMEK)
- Cloud KMS for key creation, rotation, tracking, and deletion
- Automatic access logging
- Passwords are hashed and salted
- Application credentials in Secret Manager
- Token-based authentication with revocable access scopes

4.2 Data in transit

Various methods of encryption are used, both default and user-configurable, for data in transit. The type of encryption used depends on the OSI layer, the service type, and the infrastructure's physical component^{vii}. Methods and strategies that are in use or can be used are TLS, BoringSSL,

Google CA, root key migration and key rotation, service-to-service authentication, integrity, and encryption.

All connections with System services are encrypted and served through TLS version 1.2 and above. You cannot access the service without using HTTPS. Certificates are verified on both sides by third-party authorities. Internal communication is done inside private subnets within disclosed data regions in the section 4.3.

4.3 Data region and location

System explicitly uses Europe-north^{1viii} in Hamina, Finland, as a geographic region for our infrastructure and data location for our European customers. The data region policy is set organization-wise, and our engineers cannot override it under any circumstances to prevent misconfigurations.

4.4 Ports

Most of the service communication is secured using the HTTPS protocol with TLS-encrypted traffic on port number 443.

Remote support for optional hardware, such as the Visit kiosk or Rooms display, requires opening additional network ports. These are listed in a separate section.

4.5 Domains and required network access

For networks that whitelist outbound connections, you can verify against these domain names:

- *.system.io

4.5.1 Required network access for System Visit kiosk devices

In addition to the general network requirements, the following are required to maintain a high level of support and ensure the System Visit kiosks function smoothly.

- ***.system.io**
- **ws-eu.pusher.com**
 - We use the Pusher service to deliver real-time status and version updates.
 - No personal or customer data is transmitted via Pusher.
- **bugsnag.com**
 - BugSnag service used to obtain comprehensive error details and support error monitoring.
 - Devices will function normally without this domain being whitelisted, but error recovery quality will be affected.
 - No personal or customer data is transmitted via BugSnag.
- ***.teamviewer.com, port TCP/UDP 5538 (TCP 443 fallback)**
 - Used to enable secure remote support and monitoring.
 - No personal or customer data is transmitted via TeamViewer.
- **Time.android.com and *.pool.ntp.org port 123 NTP**
 - We use this service to keep the device clock synchronized
 - No personal or customer data is transmitted via time synchronization.
- ***.eloview.com, port 8883 (MQTT over TLS), 123 (UDP – NTP)**
 - Used for OTA updates, device provisioning, remote monitoring, and general device support
 - Additional required URLs for Eloview:
 - ***.1e100.net**
 - ***.us-west-2.compute.amazonaws.com**
 - **https://cognito-identity.us-west-2.amazonaws.com/**
 - **https://cognito-idp.us-west-2.amazonaws.com/**
 - **https://polaris-promote-prod.s3.us-west-2.amazonaws.com**
 - **https://polaris-scan-prod.s3.us-west-2.amazonaws.com**
 - **eloproduct.blob.core.windows.net**

- No personal or customer data is transmitted via EloView.

4.5.2 Required network access for System Rooms devices

- *.system.io
- Time.android.com, port 123 NTP
 - We use this service to keep the device clock synchronized
 - No personal or customer data is transmitted via time synchronization.
- ws-eu.pusher.com
 - We use the Pusher service to deliver real-time status and version updates.
 - No personal or customer data is transmitted via Pusher.

4.6 Uptime and reliability

We constantly monitor our service performance and have automatic notifications to ensure a rapid response to service interruptions. Our commitment to reliability includes:

- Code quality: All code is tested, audited, and approved by at least two engineers before being deployed to production services.
- Security vigilance: We monitor updates from the security community and update our systems when vulnerabilities are discovered.
- Infrastructure resilience: Our systems leverage Google Cloud's global network with redundant systems across multiple availability zones.
- Performance optimization: We utilize Google Cloud's load balancing capabilities to distribute traffic and maintain performance during high-demand periods.
- Scalability: Our deployment architecture takes advantage of Google Cloud's autoscaling features to handle varying workloads efficiently.

5 Application

5.1 Authentication

Password authentication is available by default to end users and validated by entropy to restrict weak passwords. Users registering through SSO use JIT provisioning.

5.2 Development process

New features, performance improvements, and bug fixes are deployed continuously. While agile continuous deployment and continuous integration, our development cycle relies heavily on a strict system for code quality and security. All codes are peer reviewed and require multiple levels of acceptance in testing and staging environments before deployment on production.

- Changes are checked for security and errors via unit, integration, and static analysis tests.
- Production data is separated from development environments.

The diagrams below will give you an overview of the System service architecture and the operations pipeline.

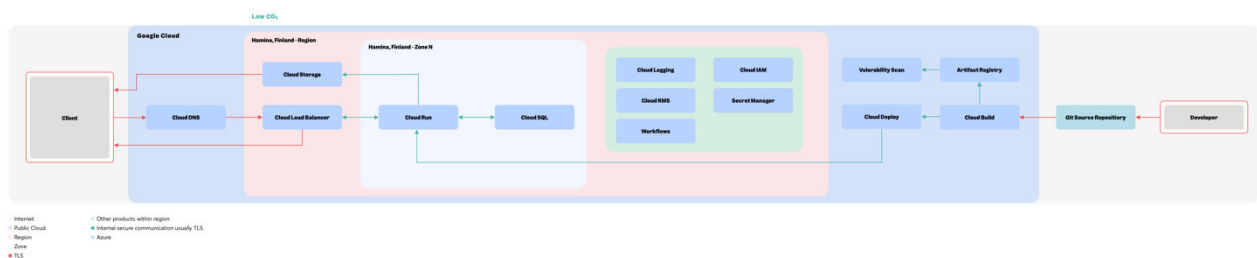


Figure 3. System development process

5.3 Audit trail and logs

System stores a read-access log of who has seen whose personal data. The user can see their limited log through their profile. System-level log is maintained. Logs have multiple levels from informational to critical and technical. Logs that could potentially have personal information are anonymized.

6 Employee access, confidentiality, and data security

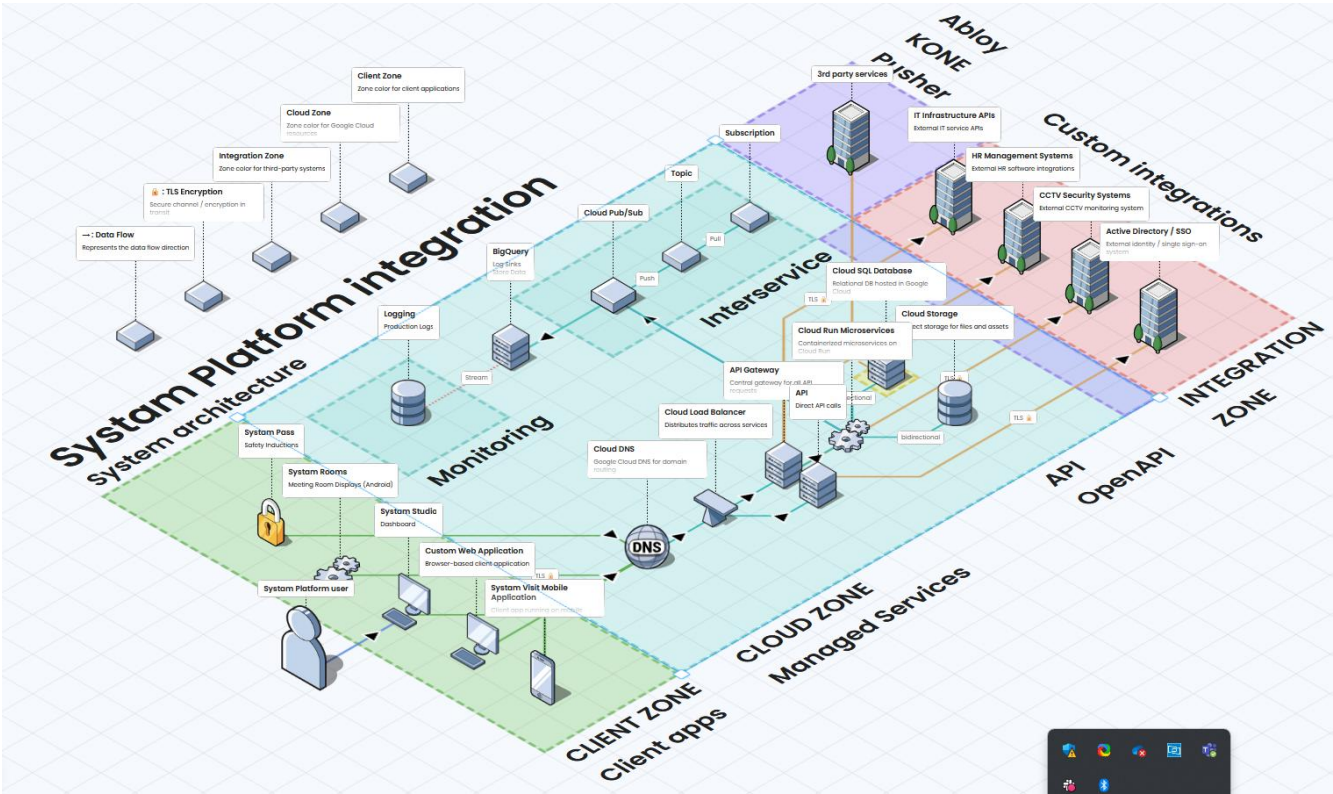
- All employment contracts for System include a confidentiality clause concerning the information of customers and partners, or they have signed a separate sanctioned confidentiality agreement.
- Customer data access is governed by our documented security policies and is limited to a small set of employees as required for support and maintenance.
- Individual employee access follows the principle of least access, and access rights are reviewed periodically.
- All employees are required to use two-factor authentication (2FA) and strong passwords that are unique from other services.
- Access is further limited to a small whitelist of IP addresses via VPN and requires public key authentication.
- Information is not passed on to third parties and is not used, for example, for marketing purposes.
- The customer can request a complete list of people who have access to their service. The list also shows the duties of these persons in System and the reason for granting access.

7 Use of sub-processors in service delivery

Systemam maintains the service itself, but the service environment's technical aspects, such as hardware and networking, are maintained by subcontractors.

An up-to-date list of sub-processors is maintained in a separate file.

8 System platform



9 Appendix

9.1 List of abbreviations

AES	Advanced Encryption Standard, also known by its original name Rijndael.
SQL	Structured Query Language
IAM	Identity and Access Management
KMS	Key Management Service
TLS	Transport Layer Security
CA	Certificate Authority
HTTPS	Hypertext Transfer Protocol Secure
JIT	Just In Time
DNS	Domain Name System
CMEK	Customer-managed Encryption Keys

9.2 General info and guidelines

- https://vm.fi/documents/10623/1107406/VM_35_2018_Julk_hallinnon_pilvipalvelulinjaukset.pdf
- https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_1_english.pdf

9.3 Google security whitepapers

- <https://cloud.google.com/docs/security>
- <https://cloud.google.com/docs/security/encryption/default-encryption>
- https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf

ⁱ <https://cloud.google.com/docs/security/infrastructure/design>

ⁱⁱ <https://cloud.google.com/security/compliance/pitukri>

ⁱⁱⁱ <https://cloud.google.com/security/compliance/offerings#/regions=EMEA>

^{iv} <https://cloud.google.com/docs/security/deletion>

^v <https://cloud.google.com/docs/security/encryption/default-encryption>

^{vi} <https://github.com/google/tink>

^{vii} <https://cloud.google.com/docs/security/encryption-in-transit>

^{viii} <https://cloud.google.com/about/locations#europe>