speakap

SECURITY WHITE PAPER

How we maintain the confidentiality, integrity and availability of information at Speakap

Version 4.1 - Feb 2024

TABLE OF CONTENTS

INTRODUCTION

Today, Information Security has to be at the heart of the modern SAAS organization. At Speakap, we've always held the view that our customers should own their data, and thus have always fiercely protected data privacy, so we see the increased attention on these topics as being great for all companies and consumers.

Information Security has always been an important aspect of all processes at Speakap, but as our company and list of customers has grown, the need for a more formalized Information Security Management System (ISMS) became more and more clear.

Over the past few years, we've documented procedures and policies, setting up regular checks and audits. We've also reviewed our systems and assets and assigned owners with specific, documented responsibilities. Finally, we've introduced a risk assessment procedure, which helps us to direct our efforts when it comes to improving and implementing information security controls.

Having an ISO 27001 compliant management system helps us to comply with regulations such as GDPR, but it also ensures that we fulfil our contractual obligations with clients and suppliers.

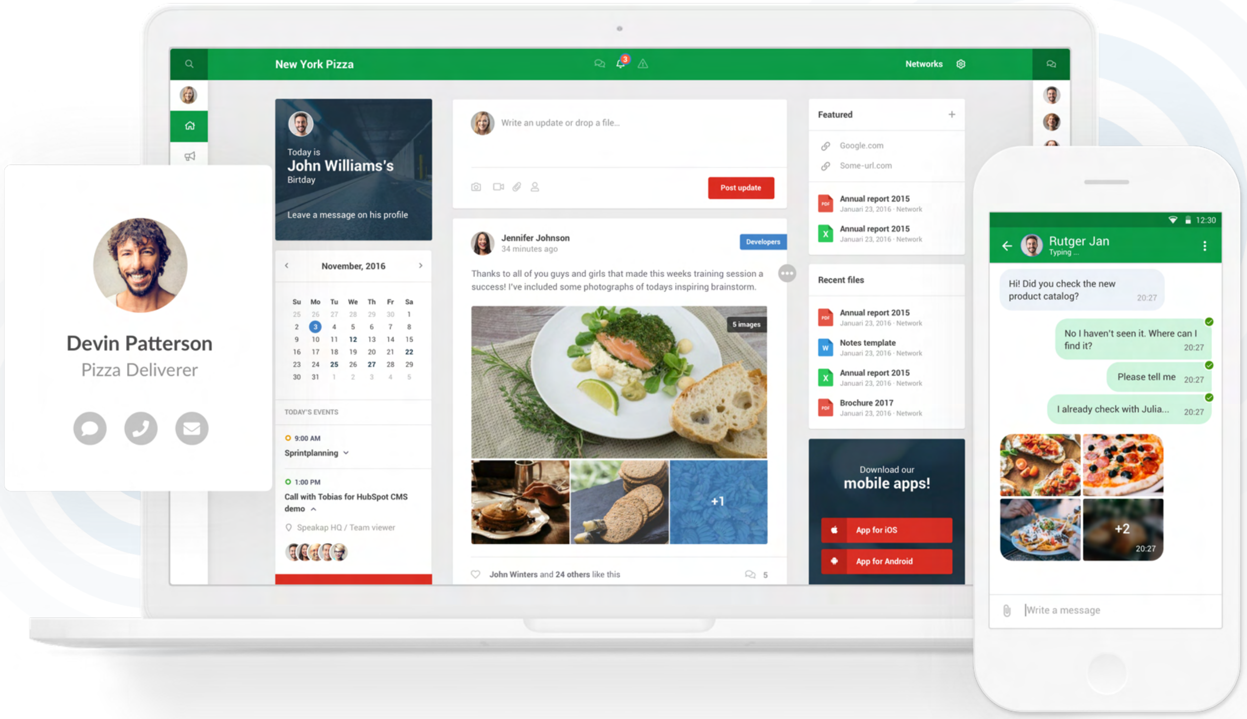
On the following pages, you will find a summary of all the organizational and technical measures that Speakap has taken in relation to information security.

> *Our risk-based approach allows us to continuously improve information security in the areas where it matters the most.*
>
> **Bart van Wissen**
> CTO

Application security

Speakap ensures that users of the platform have access to precisely the data which they are authorized to access. The security model of the application is based on:

- Users: the members of your organization, managed by designated administrators within the organization. All members of the organization (the 'network') have a role which determines the users' rights at the network level.
- Messages: Shared privately in private messages, meaning only sender and recipient have access, or shared with a group or with the entire network.
- Timelines on which data can be shared in the form of messages.
- Groups with memberships managed by designated administrators within the group or at the organization level. All members of a group have a role within that group, which determines their privileges. Groups have their own timelines, and content shared in the group (depending on the type of group) is only accessible to members of the group.



Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Thanks to all of you guys and girls that made this weeks training session a success! I've included some photographs of todays inspiring brainstorm.

Hi! Did you check the new product catalog? 20:27

No I haven't seen it. Where can I find it? 20:27

Please tell me 20:27

I already check with Julia... 20:27

Web security

- All connections to and from the service use https with the TLS 1.2 protocol, using 2048 bit RSA keys and AES encryption, provided that clients support this as well (most modern clients do).
- The older and weaker SSL protocol is disabled.
- Sensitive cookies are set with secure- and HTTP-only flags.
- All user input is validated before processing. Special care is taken to prevent Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) and SQL Injection.

Malware Protection

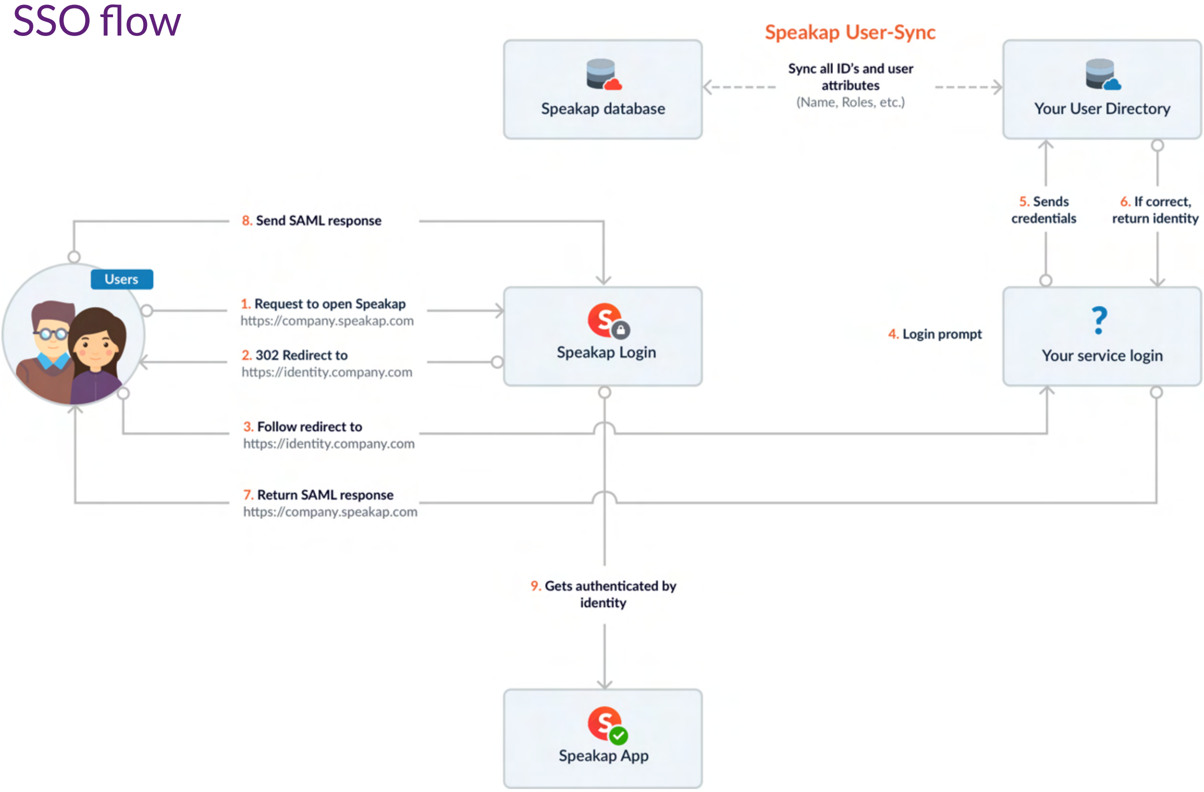
- User-uploaded files are automatically scanned for malware upon upload and rejected if malware is found.
- Malware definitions are updated regularly and automatically.

Authentication and Passwords

- Speakap API Authentication is based on OAuth 2.0. Access tokens have a length of 100 bytes, generated using OpenSSL's pseudo-random byte-string generator and have a lifetime of 1 hour, after which they need to be refreshed.
- All active access tokens are revoked when a user changes his or her password.
- SAML 2.0 can be used for Single Sign-On.
- Devices can be logged out remotely.
- Passwords have a minimum length of 10 characters, must contain at least one lowercase character, one uppercase character, and one non-alphabetic character.
- Passwords are stored as salted hashes using the BCrypt algorithm, so Speakap has no knowledge of the actual passwords.
- In order to change a password, a user must always provide the old password.

- When a password is forgotten, a user can request a password reset. A secret link to reset the password is sent to the user's primary email address.
- Email addresses need to be verified using a secret token before they can be used as primary email address.
- Passwords are never stored on the user's device or in the browser. Instead, an OAuth token is stored securely.
- The token is cleared on mobile devices when the user logs out or uninstalls the app.
- Authentication tokens expire automatically when not used for a longer amount of time.

Speakap SSO flow



Encryption

- Data is encrypted in transit and at rest.
- All communication over public networks uses HTTPS with TLS 1.2 (where supported by the client). RSA keys have a length of 2048 bits.
- The older, weaker SSL protocol is disabled.
- Customer data is encrypted at rest using the AES-256 algorithm.
- Passwords are stored as hashes, using the highly secure BCrypt algorithm.

Email Protection

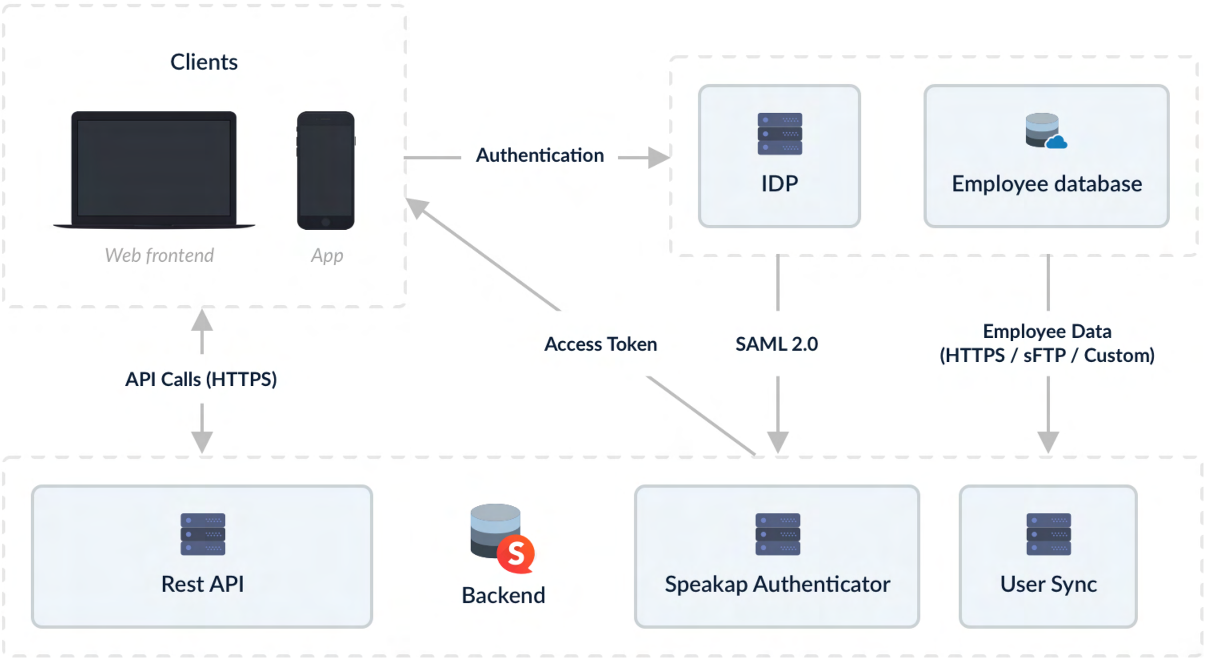
- Outgoing transactional email is handled by our ISO 27001:2013 certified email delivery partners: Tripolis (for customers hosted in the EU) and Amazon Web Services (for customers hosted in the US).
- DKIM signing is applied to all outgoing email.
- Sender forgery is prevented using SPF.

Protection of Servers and Infrastructure

- The production environments are divided up into multiple secure zones with firewall rules protecting traffic between them.
- Access to the production environments requires a VPN connection with mandatory 2-factor authentication.
- A limited group of senior system engineers has access to the servers in the production environments.
- Least-privilege principle is applied.
- All services are protected by firewalls.

- On all servers, all ports and services are blocked by default and only opened when services are required.
- Speakap servers are provisioned using a centralized configuration management system which ensures unified secure configuration across all servers. Version control is applied to all configuration data.
- Security-critical patches are installed within 24 hours of availability.
- Speakap servers are automatically protected against DDoS attacks.

Speakap
Architecture overview



Logging and Monitoring

- Operations performed by users in the application are logged to a centralized audit log.
- Server logs which are relevant to security are stored in a centralized way and are subject to analysis and automated alerting.
- 24/7 monitoring and automated alerting ensure Speakap system engineers can act quickly in case of service disruptions.

Disaster Recovery, Backup and Redundancy

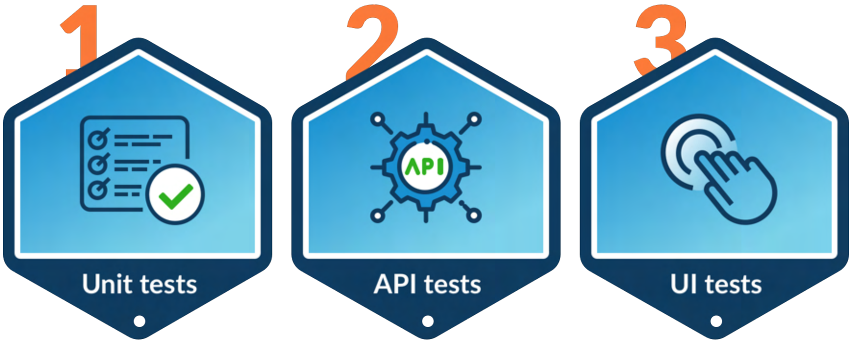
- Speakap guarantees 99.8% uptime, excluding scheduled maintenance windows.
- All critical services are set up redundantly to ensure high availability, in most cases with fully automatic failover.
- All customer data is backed up multiple times a day and kept for one month so that data can be restored in case of an emergency.
- Encrypted backups are stored off-site. For customers hosted in the EU these are stored in a separate data center located in Germany. For customers hosted in the US, these are stored in a separate AWS availability zone.
- Speakap's disaster recovery plan helps to quickly recover services in the event of a disaster.

Data Centers

- The data centers in which Speakap is hosted are ISO 27001:2013 certified.
- Speakap’s backend systems are hosted primarily at Amazon Web Services, with data centers located in Europe for European customers, and in the United States for U.S. customers. For European customers, additional infrastructure is hosted at Leaseweb in The Netherlands.
- Customer data resides either in the EU data center or in the US datacenter. There is no transfer of data between these and the customer is in full control of the geographical location of the data.
- Physical access to data centers and servers is restricted to authorized data center personnel.

Security during Development

- Speakap development environments are separated from testing and production environments.
- Production data is never used for testing purposes.
- Production data is never transferred out of the production environment to test environments.
- Automated test suites are run for every change to Speakap code, and changes are not deployed until all tests pass. In addition, manual testing and quality assurance are done in an isolated testing environment that is not accessible to normal users.



- All changes to Speakap code are peer-reviewed by senior developers who have extensive knowledge of application security. The application is developed according to industry best practices and measures are taken to prevent vulnerabilities such as those listed in the OWASP Top 10.

Security Audits, Penetration Tests and Automated Tests

- At least once a year, a series of penetration tests is carried out by an external independent security firm.
- In addition, a Security Bug Bounty program is run, facilitated by an ethical hacker platform.
- Daily automated SSL server tests ensure our SSL configuration stays up to industry standard.
- The access controls of the application are subject to automated tests which are run on every change and every release.
- All changes to the application are subject to an extensive suite of API and integration tests as well as unit tests and static analysis.
- Customers are permitted to conduct their own penetration tests on request.

Organization and Management

- Risk assessment and business impact analysis are carried out regularly.
- The ISMS is audited both internally and externally on a yearly basis as required by the ISO 27001:2013 standard.
- Information Security Awareness training ensures awareness of security risks and controls among all personnel.
- Personnel with access to customer data is screened prior to employment.
- Developers are required to demonstrate in-depth knowledge of security topics prior to employment.
- To protect sensitive data, Speakap employees sign a non-disclosure agreement upon employment.
- Clean desk and clear screen policies ensure confidentiality at the Speakap offices.
- Employee workstations are required to have strong passwords, full-disk encryption and automatic screen-lock.
- Speakap's Password Policy requires that employees use strong, unique passwords for all systems used and that additional measures such as 2-factor authentication are applied when possible.
- Information classification policies, together with documented information and asset handling procedures ensure confidentiality, integrity and availability of sensitive information.
- All policies have identified owners and are reviewed regularly.
- Access Management procedures ensure that employee access to systems is granted and revoked when changes occur, such as onboarding, changes in roles within the organization or termination of employment.

Incident Response

- Speakap has a documented Information Security Incident Response Procedure to ensure that responsibilities are clearly defined and the correct actions are taken in case of security incidents.
- Speakap has a documented Personal Data Breach Notification Procedure which ensures that the correct people are notified in accordance with GDPR articles 33 and 34.

Compliance

- Speakap maintains an Information Security Management System and is ISO 27001:2013 certified.
- Speakap is NEN 7510 certified, making our platform available for the health sector.
- Speakap is GDPR compliant.
- Speakap has undergone a successful SOC 2 Type II audit by an independent auditor regarding the design, implementation and operational effectiveness of the internal control measures.
- Speakap is HIPAA compliant by meeting the requirements of the HIPAA Security Controls.
- Data Processing Agreements are in place with all sub-processors.
- Speakap has appointed a Data Protection Officer (DPO).
- Speakap will direct law enforcement requests to the customer unless legally prohibited, so that the customer can decide whether to produce the requested information or oppose the request.

speakap

www.speakap.com