Buildsimple

Data Privacy

René Weseler

Münster

15.01.2019

Data Privacy aspects

Secure
API’s

Secure
data processing

Secure
data storage

GDPR
compliance

Certificates

Secure API‘s

Your data is secured via a SHA encryption and documents are securely processed in the corresponding AWS region

Today available regions

Europe: Frankfurt am Main
US-West: Virginia

Each API call is SSL encrypted and only accessible via HTTPS

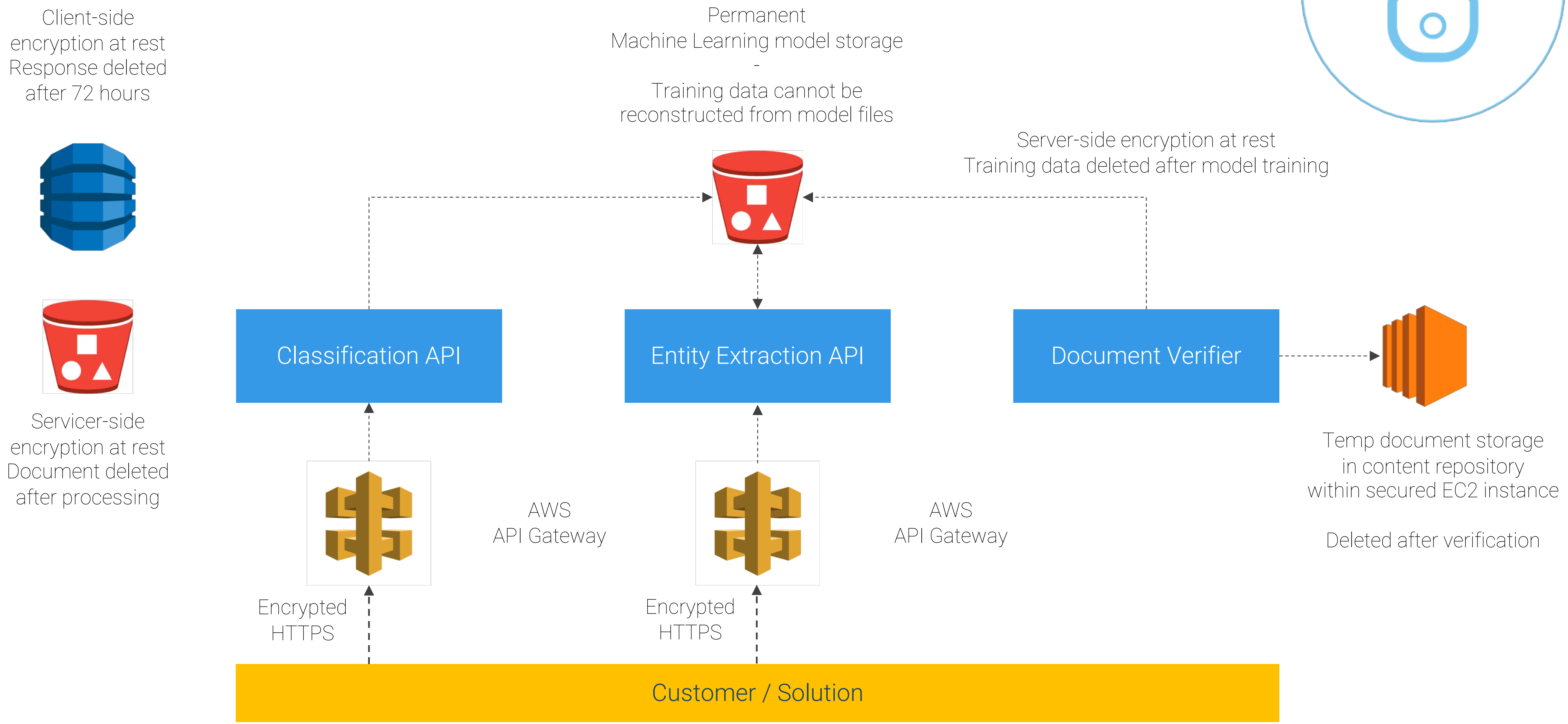
We are using AWS API gateway which provides a wide range of security features. The Amazon API Gateway performs all tasks for accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, API version monitoring and management.

We use AWS Identity and Access Management (IAM) to authorize your access to our services.

https://aws.amazon.com/de/api-gateway/faqs

Buildsimple

Secure data processing



Client-side
encryption at rest
Response deleted
after 72 hours

Servicer-side
encryption at rest
Document deleted
after processing

Permanent
Machine Learning model storage
-
Training data cannot be
reconstructed from model files

Server-side encryption at rest
Training data deleted after model training

Temp document storage
in content repository
within secured EC2 instance

Deleted after verification

Secure data storage

Runtime data deleted after processing

The data is stored in secured AWS DynamoDB and S3 buckets for the processing lifetime and deleted after the document was processed.

The classification and entity extraction results are stored in encrypted DynamoDB tables, only accessible for the corresponding customer and is deleted after 72 hours.

Training data

The training data for continuous training of the machine learning models is stored as long as the models have not been trained with the new training data. After the training, the training data is deleted.

The former trained information of the permanent machine learning models is not reconstructable out of the machine learning models.

GDPR compliance

All of our services are developed and managed GDPR compliant

Each customer signs a standardized or specific data processing agreement with Buildsimple.
This agreement contains the list of processed personal information and the information of the processing supplier chain.

After a customer unsubscribes from Buildsimple services, all information is deleted automatically and completely.

Additional available documents

ISR Security Whitepaper
IT Service Continuity Management
List of procedural instructions

General data protection regulation

Buildsimple

Certificates

AWS Well-Architected

"Security" of the Well-Architected-Framework deals with the protection of information and systems.
Key issues include confidentiality and data integrity, rights management including setting and managing individual permissions, protecting systems, and establishing controls to detect security incidents.

ISO 27001 (work in progress)

The international standard ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements specifies the requirements for setting up, implementing, maintaining and continuously improving a documented information security management system taking into account the context of an organization.

In addition, the standard includes requirements for the assessment and handling of information security risks according to the individual needs of the organization.

Cloud Security Alliance STAR Self Assessment (work in progress)

CSA STAR Self Assessment is free and open to all cloud providers and allows them to submit self assessment reports that document compliance to CSA-published best practices.