

TA/UTAX Cotopat:

Security White Paper

Revision History

Release Date	Revision	Chapter	Revised content
2026/07/01	1.0	Total	Creation of the first edition

Contents

1.	INTRODUCTION	III
1.1.	About This Document	iii
1.2.	Audience	iii
1.3.	Abbreviation	iii
1.4.	Trademarks	iii
2.	SYSTEM OVERVIEW	IV
3.	USER IDENTIFICATION AND AUTHENTICATION	V
3.1.	Account Lockout Policy	v
3.2.	Password Policy	v
3.3.	Automatic logout	v
4.	TECHNICAL DETAILS ON DATA PROTECTION	VI
4.1.	Protecting data at rest	vi
4.1.1.	Access control	vi
4.1.2.	Authentication	vi
4.1.3.	Encryption	vi
4.1.4.	Data Backup	vi
4.2.	Protection of Communication Data	vii
4.3.	Secure communication between server and database	vii
4.4.	Security Vulnerability Diagnosis	vii
5.	GOOGLE CLOUD PLATFORM SECURITY TECHNICAL DETAILS	VIII
6.	CONTACT	FEHLER! TEXTMARKE NICHT DEFINIERT.

Introduction

1.1. About This Document

This document is confidential. Please keep it for internal use. This document itself cannot be distributed outside the Kyocera Document Solutions Group, such as to channel partners or end users. Dealers can use the contents of this document to create a new public document for their dealerships and make it available outside the Kyocera Document Solutions Group, such as to channel partners and end users. This document contains information about KYOCERA Cotopat as of August 2025.

1.2. Audience

This document is intended for the readers of RHQ and sales companies of the Kyocera Document Solutions Group.

1.3. Abbreviation

- TA stands for TA Triumph-Adler.
- GCP stands for Google Cloud Platform.

1.4. Trademarks

Cotopat is a registered trademark of KDC.
Google Cloud Platform (GCP), Google Chrome, and Android are registered trademarks of Google Inc.

All other brand and product names used herein are registered trademarks or trademarks of their respective owners.

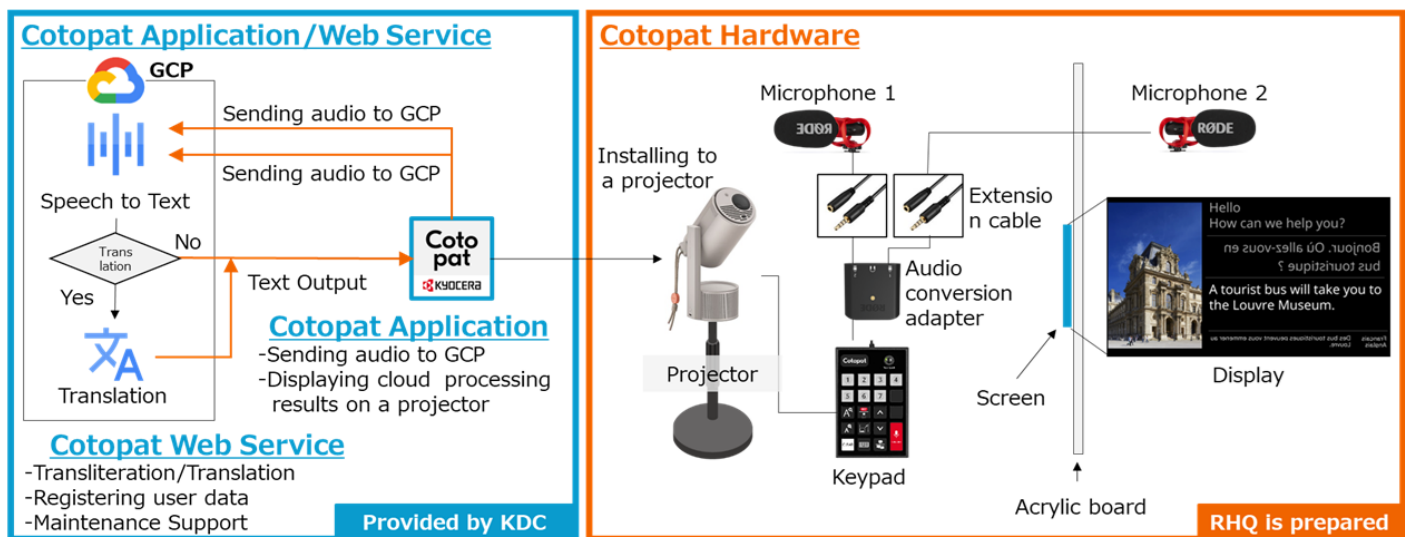
2. System Overview

Cotoppat is a system that recognizes spoken words and displays text, graphics and videos in real time to facilitate communication.

In particular, it can solve communication problems with hearing-impaired people, elderly people and foreigners who have communication concerns. This allows customers to have a safe conversation while watching the other person's facial expression, and allows the customer to communicate information smoothly, thereby contributing to improved customer service and shorter response times.

Cotoppat has the following system configuration:

- **Cotoppat Application:** Recognizes your microphone audio in Google Cloud Platform (GCP) and displays the translation results.
- **Cotoppat Web Service**, which can perform speech recognition and translation operations and register the data that customers want to see in the Cotoppat Application.
- **Cotoppat Hardware** is a set of hardware for captioning.



This document covers Cotoppat Application and Cotoppat Web Service.

Cotoppat was developed by Kyocera Document Solutions (KDC) and Kyocera Document Solutions Development Philippines (KDDP), all of which are certified to ISO 27001.

3. User identification and authentication

To access the Cotopati Web Service, the user must log in with a valid account. Unauthorized users cannot access the Cotopati Web Service. The following login security features are supported:

3.1. Account Lockout Policy

The account lockout policy protects Cotopati Web Services from password cracking attacks. If a user fails to log in a certain number of times in a row, the user account is locked out for a period of time.

The table below shows that an account is locked out after 5 consecutive failed login attempts, and the account is unlocked after 60 minutes.

Number of consecutive login failures	Five times.
Automatic unlock time	60 min

3.2. Password Policy

The user must set a password that meets the Cotopati Web Service password policy and is difficult to parse.

The setting of a password that does not meet the password policy is prohibited. This prevents users from setting simple passwords and prevents unauthorized access by third parties.

The Cotopati Web Service does not store the password itself; it stores the hash value of the password in a database. By storing only the hash value of the password, a user's password cannot be exposed even if a copy of the database is exposed. Each time a user enters authentication information, the password entered is hashed and compared to the hash value of the password stored for that user for authentication.

The browser also masks all passwords in the password field, preventing nearby people from casually reading your password from the screen.

The password length and complexity are defined as shown in the following table.

Password length	8 ~ 50 characters
password complexity	Use at least one letter from each category: - the number 0 ~ 9 - Uppercase letters * - Lowercase letters * - Special Symbols (! " # \$ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { } ~) *English alphabetic characters only (Do not use Unicode characters such as umlauts and Japanese kanji/hiragana/katakana.)

3.3. Automatic logout

An automatic logout feature is implemented to prevent users from logging in but leaving the device unused. Users are automatically logged out when it detects that their login session has become idle.

4. Technical details on data protection

This chapter is intended for those with technical knowledge.

4.1. Protecting data at rest

Critical Cotopac Web Service information assets must be protected and must not be compromised or lost. Cotopac Web Services provides security protection for stored data and data recovery through the following features:

4.1.1. Access control

Cotopac Web Service environment resources are limited to individuals who maintain and monitor the environment (Referred to as “operators ” for IT Ops, DevOps, etc.). Only properly access-controlled operators can access Cotopac Web Service's GCP environment resources. The operator must be granted the appropriate role-based access control (RBAC) permissions.

4.1.2. Authentication

User authentication is required to access data in the Cotopac Web Service database. Authentication credentials are generated from the user account issued at the time of Cotopac purchase.

4.1.3. Encryption

Only when using the conversation recording, the text data converted from voice to text, the image/video data displayed during the conversation recording, and the summarized text data are saved on Cotopac Web Service.

Except in the above cases, no data (Audio data and text data) is stored on the Cotopac Web Service. They are also not stored in the projector's non-volatile memory.

Communication between the application and Cotopac Web Service supports the HTTPS secure protocol (TLS 1.2), which encrypts data for secure communication.

4.1.4. Data Backup

Cotopac database backups are performed automatically every day. The backups are encrypted with AES256 and stored in Google Cloud Storage. The retention period for backup data is seven days.

The backup data is stored in secure locations that are separated from the primary hosting environment and is replicated across multiple locations to meet geographic redundancy and disaster recovery requirements. In addition, the data is distributed and stored redundantly across multiple regions within the applicable area, ensuring that it can be restored even in the event of a hosting environment failure or a regional disaster.

The following data is backed:

- Preferred terms
- Highlighted terms
- Custom terms
- Visuals
- Logos
- Signage
- Conversation record

The deployment and database backup regions are as follows:

RHQ	Backup region name	Explanation of the Backup region
KDEM/TA	eu	Data centers in the European Union

4.2. Protection of Communication Data

Cotopat Web Services uses proven GCP.

When you access Cotopat Web Services, you can verify your identity with two-step verification and then check your words, image and video settings, as well as your conversation records.

Kyocera Document Solutions cannot refer to the information displayed on the display such as the customer's words, images, video data and conversation records.

Kyocera Document Solutions will not be able to refer to your changed password. (password hidden)

4.3. Secure communication between server and database

Port number 443 is used for TCP communication. Please leave the above port open when using your Wi-Fi environment.

4.4. Security Vulnerability Diagnosis

To ensure the level of security of Cotopat Web Services, vulnerability assessments are conducted by external experts.

5. Google Cloud Platform Security Technical Details

Cotopat is hosted on the Google Cloud Platform. GCP meets the broad set of internationally recognized information security controls and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1/2/3, GDPR, CCPA (see the detailed list of compliant standards in GCP Cloud Compliance, <https://cloud.google.com/security/compliance>).

The hosting environment is designed to utilize the GCP provided services and security features to help secure and monitor our application. The various features that are utilized include:

- Various GCP credential for login/access
- Security logs
- Instance isolation
- Firewalls/API access
- Secure HTTPS access points
- Network security (VPC isolation, Network Security groups, Network Access Control List, Internet Gateway, etc.),
- Storage
- Simple Notification Service monitoring Cloud Monitoring application logs

Cotopat is deployed to the following GCP datacenter:

- Belgium (europe-west1)

Google Cloud Platform Security Technical Details

- <https://docs.cloud.google.com/docs/security>
- <https://docs.cloud.google.com/docs/security/overview/whitepaper>
- <https://cloud.google.com/compliance>