Contents

Introduction

CloudCTI is a service which provides a link between business telecommunications systems and databases or applications containing data of customers and relations of the service's user. CloudCTI is hosted by Microsoft Azure data centers. This document describes how third-party data are handled and how the security of the data and the service is given shape.

Scope and purpose of security

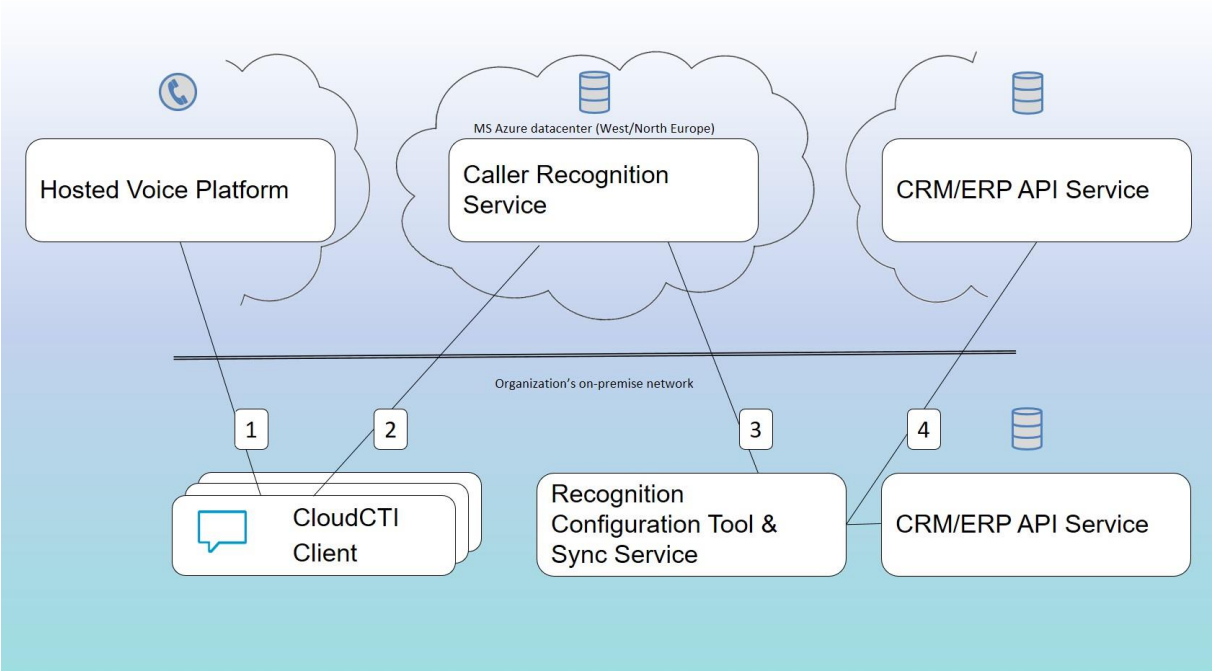
CloudCTI endeavors to take adequate technical and organizational measures to protect the personal data which are being processed against loss or any kind of wrongful processing (such as unauthorized examination, impairment, change or provision of the personal data).

A duty of confidentiality to third parties applies to all personal data that CloudCTI receives from its resellers or end-customers and/or that it collects in connection with providing the CloudCTI service. CloudCTI will not use this information for any purpose other than that for which it was obtained, even if the information has been put in a form that makes it impossible to trace it back to the person concerned.

Functionality of CloudCTI

- Click-to-dial:
  The user can start a call command in any application via numerous supporting protocols and methods. This is generally a CRM package that contains contact persons and telephone numbers, but the same is also possible via a web page that displays a telephone number. When the command is processed it is put through to the telephony platform on the basis of the settings of the logged-in user. This results in the user's telephone calling the number concerned.
- Caller recognition:
  If an inbound call is received on the user's telephone, the caller's number is indicated. Recognition of the number is requested and, if recognized, a notification displays the available information.
- ScreenPop
  The available scripts based on the caller's number are retrieved when an inbound call is received; these scripts are set up at the user's organization. If the number is recognized, the scripts generally activate the caller's data in the user's CRM application. But even if the caller is not recognized, scripts can be set up to display the CRM package with the field for the telephone number already filled in so that a new contact can be entered.

Architecture



User's environment

The CloudCTI Client (CC), the Recognition Configuration Tool (RCT) and the Synchronization Service (SS) are installed in the customer organization's environment (network). The CC is installed at every workspace that uses the service. The RCT and SS only need to be installed at one place in the organization. The SS has to be able to retrieve the contact data from there to synchronize to CloudCTI. If the organization has its CRM/ERP data on the premises the SS usually runs on the same machine.

CloudCTI datacenter's environment

The CloudCTI datacenter runs on the Microsoft Azure platform, at the locations of Western Europe and Northern Europe. The Azure platform is ISO 27001 certified. The Caller Recognition Service (CRS) is in the CloudCTI datacenter. This service serves the CloudCTI clients with the duplicated contact data from the CRM/ERP database of the user's organization (“Recognition data”). These data are retrieved from the back-end database which is in the same datacenter and is always only available for the organization’s own users.

Connections and authentication

The CloudCTI Client sends call commands to the Hosted Voice Platform and receives indications for inbound calls via connection 1. Although each platform manufacturer’s API is different, the connections are secured on the basis of TLS. The CloudCTI Client then retrieves the information relating to the caller's number via connection 2. This connection, as well as connections 3 and 4, are secured using TLS using minimally version 1.2. and strong cipher suites using SHA2. As CloudCTI keeps up with the latest security standards in general, naturally the endpoints are currently being updated and will all use TLS 1.3 within 2025 (some public API endpoints take longer because partners may need time to adjust).

The recognition data's retrieval by the Synchronization Service is also done via a connection secured by TLS, if the data are made available from an online source. If the data come from within the customer

organization's network, and connection 4 is thus strictly local, CloudCTI may support secured and unsecured connections. And even then, if the Synchronization Service retrieves the data locally, the service will be installed on the same machine and, in that case too, the data will not pass through the network unsecured.

Messages specifically intended for users and organizations can only be sent if the users have authenticated themselves with a username and password ("Account data"). Users can set and change their own passwords. The passwords must be at least eight characters long and must include at least an uppercase letter, a lowercase letter, a digit and a special character (#?!@$%^&*-).

Storage and management of data, personal details and source code

Users with the appropriate authorization set up the link to one or more CRM/ERP applications in the Recognition Configuration Tool. These settings are stored in the CloudCTI datacentre and are only available to those users. The Synchronization Service uses these settings to export all the telephone numbers from the sources that have been set, plus all the fields that (1) have been set to be displayed in the notification (such as caller's name, company's name, etc.) and (2) fields that have been set as a parameter for scripts (such as customer numbers). No other field whatsoever is processed by the Synchronization Service, stored or sent to the CloudCTI datacentre. A hash is stored locally for each telephone number plus associated relevant information, so that changes can be detected efficiently in subsequent synchronizations and the Synchronization Services only need to forward the changes concerned to the CloudCTI datacentre.

The data that the Synchronization Service sends to the CloudCTI datacentre (Recognition data) contain information that can be traced back to individual persons. These data are only stored within the European Union and the data storage is therefore not geographically redundant storage (only Azure location for Western Europe). However, to ensure reliability and availability, three copies of the data are stored, but only in the same local unit (locally redundant storage). The databases are not accessible from the public Internet, nor is there an API link that provides direct access to the data concerned. CloudCTI stores these personal data in accordance with European and/or Dutch privacy legislation.

If a user discards the link to his CRM/ERP application in the Recognition Configuration Tool, the recognition data are immediately deleted too. All recognition data are also immediately deleted if the relationship with the customer organization is ended. Administrative data relating to the user are also deleted after seven years.

If a user reports a problem, the user's activities may be temporarily logged. These logs may also contain personal data and are only stored in the CloudCTI datacentre. These logs are only accessible to appropriately designated Keylink employees with a contract that includes a duty of confidentiality clause. When the ticket for the report is closed these logs are deleted.

Lastly, the source code is stored locally and partly by Microsoft's Visual Studio Team Services. This is only accessible to appropriately designated Keylink employees with a contract that includes a duty of confidentiality clause.

Storage Technical information

Type of Data: End-users CRM contact data

Encryption At Rest: Database disks are always server-side encrypted using AES 256 based data encryption keys (DEK), which are, in turn, protected with platform managed keys. For further details about the encryption process, please see https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption.

Data segregation: All end-user data is segregated by using separate database tables per customer. A customer's data can only be accessed using a valid security token for that specific customer.

Hard- and software security measures

Physical security, hardening, registration and cleaning

All systems used to deliver the service are hosted by Microsoft Azure, West and North Europe which complies with ISO 27001 to ensure physical security.
CloudCTI configures equipment according to the security guidelines of the manufacturer. CloudCTI uses the benchmarks for security and compliance centre from Microsoft Azure and only allows essential functionality on all systems. All systems have Microsoft defender active and are kept up-to-date, specifically security patches are installed within 24 hours after release on test servers and within 7 days after release on productions systems. Binary modules are scanned through the virusscanner aggragator virustotal.com for heuristics and more thoroughly analyzed upon suspision.
Microsoft does not disclose exact physical locations, but complies with ample standards and regulations such as HITRUST, ISO27001 and ISO27018 etc.
All media carrying information are completely and irrecoverably cleaned or destroyed before re-use or disposal.

Business Continuity: management, plans and back up

A Business Continuity Management (BCM) process is implemented (MSAzure, ISO 22301:2012, Certificate: BCMS659501) that identifies continuity risks for the service delivered and determines the mitigating measures (a.o. continuity plans).
Continuity plans are available, updated regularly and exercised on a regular basis and report any shortcoming. All systems used to deliver the CloudCTI service are planned and implemented according to Microsoft Azure's High Availability *) guidelines to ensure delivery according to the SLA.

Customers are notified when these exercises are planned if the exercise could have impact on the service delivered. If shortcomings are noted, an improvement plan or updated continuity plan with clearly defined actions with agreed solution terms will be drafted.

*) https://docs.microsoft.com/en-us/azure/architecture/resiliency/high-availability-azure-applications

Backups of system and application data are performed periodically and are securely stored at a different location as specified in the SLA(s). Restore are tested periodically. For security reasons, cached caller recognition data is never backed up. If this would be lost (e.g. through hardware disaster) it would simply be 're-cached' from the end user's data source.

Internal identity and access management

The following requirements regarding identity and access management of CloudCTI employees are applicable:

- For functional accounts a responsible natural person is assigned who is responsible for the use of the account
- Default accounts are disabled.
- Access to Azure resources is granted using Role Based Access Control.
- Accounts are administered in Azure Entra and authenticated based on username and password with MFA.
- Access to resources is granted to an individual based on his role only.
- Authorizations within a resource are defined and documented.
- A line manager evaluates the authorization requests of his/her direct reports.
- Each application, system and network element has an up to date administration of the current granted accounts and authorizations.
- It is verified at least annually if the granted authorizations of each employee are still needed to do their work (attestation by manager for direct reports).
- In the case of change of a position, accounts and authorizations are revoked. - When a user account is no longer necessary it is removed or disabled.

Security roles and responsibilities of each employee are addressed prior to employment and are defined and documented. Specific security roles and responsibilities are included in job descriptions and job performance cycles. During employment employees are made aware of rules and procedures concerning security and regulatory requirements.

Roles and responsibilities are defined in addenda to job descriptions, agreed upon by employees

All new employees are subject to background verification. This procedure is part of the recruitment protocol and potential employees will be made aware of this verification in advance.

Cyber Incident Response

If, despite our efforts, unauthorized access to the systems and data under our control should ever occur we aim to respond quickly, effectively and be transparent about the issue.

Suspicious behaviour is detected automatically (e.g. unusual password or API activity triggers alerts; mysterious emails is placed in quarantine) and by a vigilant workforce. Therefore, it is important to us our employees are aware of security threats and know when to contact IT.

procedure

Naturally, the top priority is to contain, deny and disrupt the threat should it be ongoing. After a full scan determines the eradication of all breeches is complete the following steps are taken.

1. Restore or repair affected systems.
2. Gather all relevant information, analyse how access was gained, mitigate found causes
3. Report criminal activity to authorities.
4. Communicate incident to relevant parties. Direct partners will be notified personally, via telephone and/or email. End-users will be notified via newsletters and/or website.
5. Review and evaluate process.