Author	Privacy department (Zucchetti S.p.A.)/ Development manager
Approval	Management

Versione Revisione

Version	Author	Consultation of DPO	Issuance date	Reason for the revision
0	Privacy department (Zucchetti S.p.A.)/ Development manager	20/05/2025	21/05/2025	First Issue
1	Privacy department (Zucchetti S.p.A.)/ Development manager	29/01/2026	29/01/2026	Reference to the Android version and change of registered office address and Z Holding Spa added as DPO.

OPINION OF DPO
OK

APP SIDE

DATA PROCESSOR						
Name	Zucchetti Axess S.p.a.					
VAT no.	03537610960					
Address	Piazza Mino Zucchetti, 1					
City	Lodi	**Postal code**	26900	**Prov.**	LO	
Legal representative	Domenico Uggeri					

ORGANISATIONAL STRUCTURE			
Division	XATLAS	**Division Manager**	Domenico Uggeri
Area	XATLAS	**Department Manager**	Marco Marchetti

PERSONS IN CHARGE OF PROCESSING
Analysis, development, quality control, and help desk staff

CONTACT DATA			
Data Processor	Zucchetti Axess Spa	Ufficio.privacy@zucchetti.it	0371.5947000
Representative of Data Processor	N/A		
Data protection officer (DPO)	ZHolding SPA	dpo@zucchetti.it	0371.5943191

DESCRIPTION

SIDE is the Axess TMC mobile application, available for iOS and Android, that allows you to clock in and open doors, turnstiles, and gates via smartphone, using *Axess TMC* terminals equipped with a BLE (Bluetooth Low Energy) reader.
In addition to employees, **SIDE** can be used by visitors for self access without having to go through a reception desk.
All *Axess TMC* terminals and controllers can be equipped with a BLE reader, featuring a TTL serial interface, allowing users to identify themselves via smartphone.

When installed on a smartphone, SIDE app automatically generates a unique code that will be sent to the *Axess TMC* terminals to identify the user exactly as if it were a badge code. The user can view this numeric code, copy it, paste it, and send it to the information system managers to have it whitelisted just like a badge code. Or he can receive one or more credentials from the Credential Manager. These credentials will be uniquely associated with the user and used to identify him/her.

The SIDE app is a "wallet" of credentials. Credentials are of different types (for employees, visitors, etc.) and technologies (BLE, QR, etc.) and are used for identification. Each time SIDE is launched, the existing credentials are displayed. The user can select which one to use. In certain conditions, the selection can be automatic. If a BLE credential is selected, the user is shown a list of available BLE readers within a 10-meter radius (if there is more than one). The user chooses which reader to use to identify themselves. It is also possible to configure the app to automatically send the user code to the first available reader.

If the user selects a QR credential, the code must be shown to a dedicated scanner.

PURPOSE OF THE PROCESSING

Purpose of the SIDE App is to allow user to be identified using his personal smartphone. This allows attendance punches and opening gates in access control system using the smartphone.
The purpose of the processing is to provide support and maintenance services to the Data Controller.

CATEGORY OF INTERESTED PERSONS

Employees, collaborators, visitors

CATEGORIES OF PERSONAL DATA

There are two cases depending on whether the SIDE APP is used in conjunction with the "Entry365" Credential Manager service or not:

- App Side without registration to the Credential Manager cloud service “Entry 365”
  - Random code generated by the App Side upon installation;

- App Side with registration to “Entry 365” Credential Manager cloud service

  - Phone ID
  - To receive credentials, the user must log in to the Credential Manager with his email address as username. The email address is not stored in the app.
  - Credential(s) generated by the "Entry365" Credential Manager service and sent to the smartphone (the app side stores all credentials it receives).

Regarding geolocation:
GPS is not used. To activate the hands-free clocking feature on iOS devices, optional "iBeacon" devices have to be installed near the BLE RFID readers. These devices emit a BLE signal according to an APPLE standard. This signal acitvates the APP SIDE. The iBeacon also instructs SIDE app which reader to send which credentials to. This happens automatically when the user enters with his smartphons within an area covered by the iBeacon.
The "where I am" data is not saved or sent to the APP; the iBeacon signal is only used to activate the APP.
To use the function described above, geolocation must be enabled on the device, even if GPS is not specifically used. If geolocation activation is not enabled, the hands-free feature will not be available even if iBeacon are installed.

Note: For information on the data processing carried out by the “Entry365” Credential Manager, consult the specific processing register

CATEGORY OF RECIPIENTS TO WHOM DATA CAN BE COMMUNICATED

Other Zucchetti Group companies Subcontractors
DATA TRANSFER ABROAD
No data transfer abroad
TERMS FOR DATA DELETION
Credentials are stored in Side until the user deletes them. The user's account data are stored in Credential Manager Entry365 cloud service. The user can request the deletion of this data and the deletion of his account via the App. *Note: For information on the data processing carried out by the "Entry365" Credential Manager, consult the specific processing register*

1. TECHNICAL MEASURES THAT CAN BE IMPLEMENTED in the APP

The developer has developed and implemented secure data processing procedures consisting of security measures at both the technical and organizational levels, as well as at the support service level.

The App Side benefits from all the security measures that the user can decide to activate directly on their smartphone, such as facial recognition, fingerprint, access code, etc.

With specific reference to the App Side, the following security measures are implemented:

- Credentials received from the Credential Manager cloud service (or the random code if using the App Side without registering for the Credential Manager service) are stored on the device in encrypted format;
- The credential code is transferred to the reader using different technologies based on the credential type: BLE credentials are sent encrypted via BLE, NFC credentials are sent encrypted via NFC, and QR credentials are read by a dedicated QR code reader. Credentials based on secure QR codes are available and are periodically updated.
- All communications between the App Side and the Credential Manager cloud service are encrypted via HTTPS;
- Credential Manager databases are encrypted.
- MFA can be implemented for access to SIDE and Credential Manager.

2. DATA CONTROLLER: SUPPORT PROCEDURES

SUPPORT SERVICE METHODS

Based on the supply method, the support for Zucchetti Axess products and services is provided in the following ways:

- On-site support
- Telephone support
- Support via e-mail/web tickets
- Support by importing customers' database
- Support via remote TeamViewer and/or Meeting Webex connection
- Support via remote VPN connection
- Start-up projects and conversions

As defined in the contract, remote support includes access to the system, which must always be authorised and controlled by the Customer/Data Controller. Therefore, each access is recorded by the operator who carries it out by saving the e-mail exchange.

CONTRACTORS TO WHOM THE SUPPORT SERVICE IS PROVIDED

The support service is provided to:

- Direct Zucchetti Axess customers
- Indirect customers

The support management generally provides:

- for direct customers: telephone call or e-mail to the service department (back office/dedicated mailbox) which sends an e-mail to the support department. The call is opened on Ad Hoc;
- for indirect customers, the request is sent directly by the customer to a dedicated mailbox (support@axesstmc.com) and it is used as HDA ticketing tool.

Support is provided on both Xatlas software and hardware (firmware), as well as on video surveillance systems (whether integrated within Xatlas or not).

PROCEDURES

ON-SITE SUPPORT

Zucchetti Axess operators access the customer's structure in order to carry out training or technical maintenance/support and installation activities.
In this case, they work as if they are part of the Customer's/Data controller's structure and they adopt all the procedures required by the Customer. The Customers/Data Controllers can generate individual user names for accessing their systems or they will provide access under supervision to Zucchetti Axess appointees in order to train their staff.
If, during the support activity, Zucchetti Axess appointees need to retrieve archives or databases in order to solve reported issues, they must inform the Customer/Data Controller and formalise, even by simply sending an e-mail, the information that they have retrieved the DB with the Customer's approval. At the end of the activity at the Zucchetti AX offices, the appointee who managed the intervention will delete the data; should it be necessary to store the data for a further period of time, a specific e-mail will have to be sent to the Customer/Data Controller with the following minimum content:
"Dear Customer, we inform you that the reported issue, which required the collection of your archives, was solved. We would like to inform you that we will store the archives from our information systems for the next X days (*to be defined from time to time as the need requires it*). At the end of the agreed period, the archives will be removed from Zucchetti Axess information systems and they can no longer be restored".

TELEPHONE SUPPORT

There are no issues as far as the personal data processing is concerned. There are no transmitted data or archives and the communication is only verbal. Generally, the first contact after the customer's request for support is always made in this way, in order to define the reported issue in detail.

SUPPORT VIA E-MAIL/WEB TICKETS

In case of support via e-mail, always add the disclaimer in the message text:
"The content of this e-mail and of possible attachments is strictly confidential, it is not admissible in court and it is dedicated to the person/s to whom it is addressed. The content of the reply to this e-mail might also be known by other co-workers, who are part of the same homogenous group of the undersigned or part of other homogenous groups who are however related to the solution of the issue reported by you. If you add

attachments containing personal data to the reply message, these will be saved in the ticketing tool and/or in the e-mail attachments and stored there for 3 years. If you received this e-mail by mistake, please notify us immediately and delete it from your computer. It is prohibited to copy and publish the content of this e-mail. Any abusive use of the information contained here, by third parties or by persons who are not indicated in this e-mail, can be prosecuted pursuant to the law. We hereby inform you that in order to exercise the rights provided by article 15 et seq. from the EU Regulation 2016/679 (GDPR), it is possible to refer to the following address: ufficio.privacy@zucchetti.it".

Zucchetti Axess appointees must never have the customer's access credentials sent by e-mail (only those used and in the possession of the customer, not those generated specifically for technicians who need to connect), nor must they save them on the ticketing tool and/or in e-mails.

If a customer/partner sends the access credentials for his/her environment without a request from Zucchetti Axess appointees, it is necessary to reply them that we are not authorised to access the systems with other users' credentials because this method infringes the EU Regulation 2016/679 (GDPR). Therefore, Zucchetti AX appointees will have to request individual credentials or the connection with TeamViewer (or an equivalent tool).

Every e-mail must be signed with the first and last name of the operator who handled the Customer's issue and the information must be saved in the ticketing tool and/or in the e-mail.
Clarifications:
The disclaimer can also be added in the web tickets.
Personal e-mail addresses should not be used, as they cannot be controlled.

SUPPORT BY IMPORTING CUSTOMERS' DATABASE

If, in order to solve the issue reported by the Customer/Data Controller, it is necessary to have the database or other files or queries containing personal data transmitted, the Customer must be informed of this necessity. If the customer is not able to make the copy himself/herself and asks Zucchetti Axess appointees to do so, it is necessary to receive his/her authorisation also for the VPN connection (to be saved in the ticketing tool and/or in the e-mail).

In order to carry out this activity, it is necessary to send the customer/Data Controller an e-mail with the following content:
"Dear Customer,
in order to solve the issue reported by you, it is necessary to check your archives.
We ask you to authorise us to connect via VPN to take copies and to process them in order to solve what has been reported".

The archives will be stored for the time strictly necessary to solve the reported issue and will be deleted by Zucchetti Axess appointees at the end of the intervention.
Data must be saved in the Directory and they should not be subject to backup".

If there is the need to store the archives, it is necessary to send an e-mail to the customer, as described below:
"Dear Customer,
having solved the issues on the archives that you sent, we request the authorisation to store your archives on our infrastructure for the next _____ days. The purpose of this storage is to check for possible issues that you may report during the use of the restored archives. At the end of the above-mentioned period, we will proceed to the permanent removal of the archives. If after this period your archives are needed, we will request them again.
To this end, we request an express confirmation by replying to this message. If your reply is negative, we will proceed to the immediate deletion of your archives".

The customers' archives cannot be transmitted to work groups other than those in charge with solving the issue reported by the customer.

The only possibility to store the archives without the prior authorisation of the customer is to make them anonymous.

SUPPORT VIA REMOTE TEAMVIEWER CONNECTION

This method of connection to the customers' tools ensures privacy because:

- The connection is always requested by the customer
- The access credentials are always individual
- The customer grants us access to an environment with an authorisation profile chosen by him/her in order for us to perform support activities
- The customer can disconnect us whenever s/he wishes.

Via TeamViewer, it is also possible to grant access for the second level support to the same session opened by us. In this case, the customer has the proof as it has been provided by the tool and therefore s/he implicitly accepts this method.

If there are codes, passwords or licenses that we must add for the proper operation of the tool and which the customer is not meant to see, it is essential to use the TeamViewer function: Show black screen

It is essential to use our TeamViewer as it is licensed and customised with the entire documentation required by the law on personal data processing.

Only in exceptional cases and after a careful assessment performed by the manager and by the privacy office, it is possible to use other connection tools that operate in the same way.

SUPPORT VIA VPN CONNECTION

If the support activity must be performed via VPN or private accesses, Zucchetti Axess operators must enter the customers' systems:

- With the customer's prior authorisation
- With the credentials that must be active for the time frame needed for the execution of the requested activities
- The credentials must be disabled at the end of the activity by the Customer/Data Controller

The creation of a user name must only be requested from the customer, who must generate it individually for every Zucchetti AX appointee.

It is necessary to send an e-mail to the customer:
"In order to carry out the support activities you have requested, it is necessary to create individual access profiles for the operators who will perform those activities. To this end, it is necessary to generate those access credentials to the system."

When the customer makes the request, after the individual user name has been created:
"In order to carry out the support activities you have requested, it is necessary to enable the user name associated to me"

At the end:
“The support activity is completed. We remind you to disable the credentials in order to protect your personal data”.

OTHER TYPES OF SUPPORT

The support is also performed on video surveillance systems. When the video camera does not work, if the system is integrated within Xatlas, you intervene directly in Xatlas; in these cases, access is granted to the configuration settings or images, but only in real time and nobody ever accesses the records. If the records are not valid, support is given to the video surveillance system maintenance technicians.