Appendix A

Detailed Scope of Services

GF6 Verona – Italy
Security Works Project
(PSIM, Access, Intrusion and CCTV)

24th October 2018

Created by:

SIG EMEA
security integrators group

Security Consult and Management Services

DOCUMENT HISTORY

Current Document Status
Status: Tender Issue, **Issue:** 00, **Date:** 24th October 2018, **Author:** Edward van den Berg, **Checked By:** Johannes Meissner

Document Revision History
Revision: 00, **Description:** Tender Issue, **Date:** 24th October 2018

CONTENTS

Created by:

Security Consult and Management Services

1.0 Introduction

1.1 Project Brief

This document describes the intent of the works that are proposed for replacements and improvements to the Zalando Security Systems at GF6 Lounge in Verona, Italy.

It is intended that this document will assist the selection process for Zalando to employ a systems integrator/contractor to undertake and manage the security implementation works.

This document aims to provide vendors with a detailed scope of Zalando requirements for a new integrated platform in meeting Zalando Business Resilience (BR) requirements, accounting for Access Control, CCTV and Intruder Detection. The chosen BR platform should also have the ability to integrate/interface with Fire Alarm panels and BMS in providing critical alerts to the Zalando Loss Prevention Team (LPT). The BR platform is to intelligently interface with the entire system to view and control the system, not just receive alarms, thus providing 2-way operability. To meet these requirements Zalando have chosen Wingard Advancis as PSIM system and use Nedap Security as the access system, Honeywell Galaxy as the intrusion system and Axis cameras on a Genetec recording system with Kiwi analytics as their CCTV delivery platform. Wingard Advancis, Nedap AEOS, Honeywell Galaxy, Axis with Genetec and Kiwi is approved by Zalando Security and is installed to manage Zalando Logistic centers, Office sites and various other facilities.

Zalando will require a detailed projection of potential cost of implementation, estimated time for completion and ongoing annual costs for support & maintenance.

Further detailed system information and security standards of Zalando can be found in the separately attached **Appendix D: Annex D.8_Global Physical Security Technical Standards**

1.2 Project Status

The building and grounds have been surveyed for projecting cameras, access points, intrusion etc. Discussions have been held internally within Zalando with respect to selection of suitable systems.

This has been based upon:
a) Reliability and future-proofing
b) Zalando Security experience and recommendations
c) Flexibility
d) Possible integration/monitoring from other sites.

In consideration of the above, Zalando have opted to request tender bids from integrators / contractors for a Honeywell Galaxy Intrusion system, an Wingard Advancis PSIM system, a Nedap AEOS Access system and an Axis camera CCTV system with Genetec recording and Kiwi analytics platform.

Drawings have been prepared indicating the proposed locations of security equipment systems throughout the building and the external perimeter. These drawings represent the final required installation of equipment / hardware.

1.3 Building and Occupation

The facility consist of the perimeter plot with car parks, fencing and access gates to be monitored by Axis external IP cameras mountable on light poles, boom barriers with Nedap access readers, license plate recognition system and intercom system
The building itself consist of an office space with a 1st, 2nd and 3th floor and a logistic warehouse divided in 4 units with several floors. Office spaces as well as the warehouse require Axis internal IP cameras to be connected to the Genetec recording system with Kiwi analytics, Nedap AEOS access readers, Honeywell Galaxy intrusion devices and Intercom systems.

Important to know in the project planning is that Zalando requires the office space to be operational prior to the warehouse becoming operational.

The occupation of the office space will be normal and comparable to general office space area's with exception of the Canteen area, the area at the connector bridge based on the 1st floor and main entrance on the 1st floor, as this is where all warehouse employees will gather during change of shift and break times. The same goes for the warehouse occupancy.

Zalando contracted Jacobs as their building contractor who will / has provided all cabling required for the Intrusion system, the Access system and the CCTV system
Jacobs will also deliver and install the required CAT cable infrastructure for the Camera and access system. Camera cabling will be mounted between the camera installation point within 1m radius from the camera position and the central switch / recording position. Jacobs will terminate the CAT cables with RJ termination boxes and test the integrity of the network cable infrastructure leaving the CCTV vendor only to install and patch the camera's and recording equipment.

1.4 System Configuration & Description

1.4.1 Operation of Building & General Configuration

The building use is based on an warehouse and office environment with 24/7 working hours. Parts of the office operate within normal office hours and outside of these hours this office part is locked down armed. There is a 24/7 security guard service that will monitor the system during its 24/7 operation.

The security system shall be configured to differentiate between office working hours and office out of hours periods and the 24/7 operational part of the office and warehouse, where motion detection and door alarms generated can be set with threat levels associated with these time periods. For example motion detection triggered outside of working hours would be considered high threat level and raise an alarm whereby during normal working hours the system would ignore movements caused by the normal working environment of the office.

The security system should have the ability to be remotely monitored via the Zalando network. The system should be configured such that events generated in the access control and intruder detection system automatically generate video clips accessible via an event log with forensic capability. More detailed requirements for these systems are provided in Section 2 of this document.

1.4.2 Controller location

With the requirement for the security system to sit on the Zalando network, any controllers, switches, network nodes and devices should be located within the Zalando Technology Rooms and / or in the dedicated security equipment room and IT requirements need to be discussed / liaised with the Zalando IT team assigned.
Zalando will later on define the exact locations of these rooms, but assume that the cable runs as provided by Jacobs will be within the maximum cable run length to ensure correct cable functionality over its maximum distance.

The main CCTV recorder should be located within a rack or wall mount in the Security Equipment Room. These main panels are to be connected via the Zalando WAN to the Security Operations Centre (SOC).
The same goes for the Honeywell Intrusion main panel, the Nedap access main server / controller and the intercom main controller
The configuration of these devices would require liaison with the Zalando Business Technology (BT) team to ensure correct protocols for connection to the network.
As described in the sections below, these rooms would require access control and camera to ensure access is provided only to those with sufficient credentials.

1.4.3 External

The requirement is to have various externally fixed IP rated AXIS IP cameras located at the terrain of the building as shown on the CCTV Site plan drawing.
There are cameras to be mounted on poles, building wall mount Cameras, Intercom cameras and ANPR cameras on the external perimeter.
The vendor is to provide an IP intercom system (which interfaces with the PSIM) where the ring stations at the car and truck entrances have an onboard camera for the intercom system. The IP Intercom Answer station must be placed at the SOC.
The vendor is also to provide license plate recognition cameras for the car and truck entrances. Please ensure that the requested Kiwi analytics software in combination with the Genetec VMS can cope with the Axis 360 cameras projected and the license plate recognition cameras (de-warp, mask public areas and multiteam recording etc.)

1.4.4 Office First Floor

The main entrance is on the Office building first floor where also the reception area is situated, the connector bridge to the building is also situated on the Office building first floor.
Some parts of the first floor office spaces may be protected with motion detectors and partitioned into a separate zone for individual arming / disarming. (controlled by the SOC).
The warehouse employee change rooms are also on the office first floor. The entrance from office area into Zalando Warehouse area is protected by means of speed gates with readers and there are also readers projected on other perimeter / high secure doors.
Several cameras are projected on strategic locations to monitor the stream of people and perimeter entrances. This area will be having high traffic peaks during shift changes. There are also visitation rooms for employees who are randomly picked by the Access system, and there are more doors which are secured by means of reader.

1.4.5 Office Second Floor

The Second floor consist off the canteen and kitchen area. The second floor may be protected with motion detectors and partitioned into a separate zone for individual arming / disarming. (controlled by the SOC).
Kitchen area will be equipped with access control. Several cameras are projected on strategic locations to monitor the stream of people and perimeter entrances.

1.4.6 Office Third Floor

There is only office space situated on the office building third floor. The third floor office spaces may be protected with motion detectors and partitioned into a separate zone for individual arming / disarming. (controlled by the SOC). All offices will be equipped with

access control.

Warehouse Floor

The warehouse floor is 24/7 operational. All perimeter doors and windows are to be secured with contacts connected to the Intrusion panel. Several cameras are projected on strategic locations to monitor the stream of people and perimeter entrances.
The contacts on the loading bays etc. are mainly there for monitoring un-authorized opening of these doors (controlled by the SOC)

1.4.7 Camera's

The following schedule is provided to give an indication of the cameras required for this security system. Please also see the separate attached Camera List for more details

2.0 SYSTEM TECHNICAL SPECIFICATION

2.1 Access Control System (ACS)

The ACS must be integrated with the following systems / devices deployed at the site:
Intrusion Detection Devices (IDD)
Video Surveillance System (VSS)
By means of PSIM system

Further details can be found in **Appendix D: Annex D.8_Global Physical Security Technical Standards**

2.1.1 System Capabilities

The systems primary communication medium must be via the Zalando network

All input circuits must be fully supervised circuits (dual resistors)

All input circuits must report the following off normal conditions to the monitoring display:
- Open circuit
- Shorted circuit
- Alarm condition

Arming and disarming input points must be performed by:
- Time and day of the week specific (Time Specification)
- Manual action
- Configured actions (event driven)

Should support the following language(s):
- English
- Native

Should be capable of receiving automated personnel data imports and producing automated personnel data exports to support integration with such applications as Cross Site Access, Human Resources data feeds, and personnel termination notifications.

Must provide a log of all:

- Activities (cardholder, system operator, system generated, etc)
- Alarms
- Configuration changes with associated operator
- Response actions with associated operator

Must be capable of storing 40,000 card records

Must provide user configurable fields to allow for custom personnel data for example:

- GUID number
- Empild number
- Personnel Type
- Contractor Company Name

Must allow the user to establish and archive system backups, including:

- Automated
- Daily
- Weekly
- Monthly
- On demand

System backups must include the following:

- Database
- Reports
- Logs
- System configuration
- Portraits
- Personnel records

Must have a means to restore the system from archived backups

Must be capable of interfacing with intrusion detection devices currently on the market

2.1.2 Workstation / User Interface Software

The system should be accessible via a standard Zalando PC via Internet Explorer or similar approved web browser. Specialist terminals with bespoke software will not be considered.

2.1.3 Access Levels

Cardholder access must be based on:
- Door / Reader
- Time and day of the week (Time Specification)

Must support multiple door / card reader assignments per access level

2.1.4 Access / Alarm Monitoring

Monitoring access / alarms must provide:
- Time of alarm activation
- Location of the alarm
- Priority of alarm
- Alarm sorting based on operator selected attributes
- Cardholder portrait call-up
- Unique response instructions for each alarm
- Be capable of displaying system component status alarm notifications such as:
  - Control panels
  - Video servers
  - Communication

System should be capable of:
- Alarm routing to any or all workstations
- Alarm routing to selected workstations based on time and day
- Sending text and or e-mail messages upon alarm activation
- Logging alarm response actions

System must allow the operator to:
- Locate and track logged events such as:
  - Specific cardholder activity
  - Specific card readers / doors state changes
  - IDD activation
- Manually :
  - Lock and unlock doors
  - Pulse outputs
  - Activate and de-activate outputs

2.1.5 Graphical Maps

System must support use of interactive maps that provide:
- Ability to import drawings in common file formats
- In response to an alarm, instantly display associated map indicating state and condition of the alarm point
- Display interactive icons representing location and state of:
  - Input points
  - Output points
  - Doors
  - Logical devices
  - Cameras

2.1.6 Reports

System must be capable of generating reports based on any combination of fields within the database via an ad-hoc query tool.

System must be capable of exporting reports in one or more of the following formats:
- Text
- Excel
- Adobe PDF
- HTML

Operator must be able to retrieve selected system transactions by:
- Specific time and date selection
- Range between a start time and date to an end time and date

System must be capable of providing the following history reports:
- Alarm point state
- System alarms
- Communication failure
- Main power failure
- Panel reset
- Low battery voltage
- Panel tamper

System must be capable of providing a cardholder status report to include:
- Active
- Inactive
- Terminated
- Expired card
- Card readers accessed

2.1.7 System Field Components

Control Panel(s) must be capable of:

- Linking ACS software / server to all field hardware components (card reader modules and input and output control modules, etc)
- Providing a fully distributed processing of access control and alarm monitoring operations
- Communicating with ACS software / server via Zalando's LAN/WAN network
- Continued operations for 4 hours upon loss of primary electrical power
- In the event the panel loses communication with ACS software, it must continue to function (stand-alone / off-line operation) and be capable of:
  - Operating all internally associated event driven outputs
  - Making access granted/denied decisions
  - Buffering transaction and event information
  - Automatically uploading buffered data to ACS sever after communications restored.

Lock power supplies must:

- Continue operations for 4 hours upon loss of primary electrical power.
- Supervise primary power status and report loss of power to ACS
- Supervise battery power status (if applicable) and report low battery power to ACS

2.1.8 Cardholder Interfaces

Global Identification Badge has multiple technologies on one card. The standard technologies are:

- Mifare Desfire EV1 / EV2

ACS must support the following Nedap or HID Corporation Multi-technology Card Readers:

- InveXS 170
- ConveXS 80F

Card Readers:

- Must use hidden or tamper resistant mounting screws
- Must provide audible signal when card is presented
- Must support Mifare Desfire Format
- Should have a read range greater than three inches
- Should contain LED status indicator
- Should contain tamper detection output
- Should be of potted construction for superior weather resistance

2.2 Intrusion Detection Devises (IDD)

Intrusion Detection Devices which interface with the ACS are preferred.

Further details can be found in **Appendix D: Annex D.8_Global Physical Security Technical Standards**

Devices must support the following:

- Low battery indicator
- Device tamper indicator
- Loss of communications status

Door Position Switches must:

- Be mounted on the protected side of the door with no exposed cabling
- Provide detection of movement of door 3” (7.5cm) or less from the closed position
- Be installed on doors and any door leaf associated with monitoring purposes
- Be installed on all Zalando perimeter doors.
- Not be magnetic bond sensors or lock sensor technologies

Please note in the office space all window and door contacts have already been delivered and installed, the cable ends above ceiling and needs to be terminated from that point onwards

Motion Detection must be one of the following technologies:

- Dual-technology where required, (otherwise passive infrared)
- Class 2
- Detection range of minimal 12x12m

Please allow for 360 ceiling detectors where feasible (i.e. in the server rooms)

Duress and Panic devices:

- Should be of a push button design and located in such a way prevent accidental activation

Glass break Detectors should be:

- Dual-technology (flex and audio)

System must be operational through Arm/Disarm Keypad as well as through a Software platform communicating over IP to the IDS
System must have audible and visual alarm notification placed on strategic locations

Any suggestions over and above the current design are welcome.
Basic system cabling will be delivered and installed by others.

2.3 Video Surveillance System (VSS) / CCTV

Further details can be found in **Appendix D: Annex D.8_Global Physical Security Technical Standards**

2.3.1 Recording Devices

Network Video Recorders (NVR) must:

- Integrate with ACS. We request you to offer Genetec
- Support unique user IDs and passwords.
- Support linkage of video clips to associated ACS alarms
- Be capable of video motion detection
- Be capable of pre and post-alarm per camera
- Allow for centralized:
  - System administration
  - Monitoring
  - Video archiving
- Accept commands from ACS to perform actions such as:
  - Marking video clips
  - Playing live or recorded video
  - On-screen Pan Tilt Zoom (PTZ) control
  - Selecting PTZ camera presets
- Provide proper sized storage capacity based on:
  - Number of channels (cameras)
  - Retention period (minimum of 30 days)
  - Allow 50% over-capacity
  - Frames per second per camera (minimum of 7.5 fps)
  - External NAS storage allowed preferably on a Synology NAS
- Provide search and retrieval capabilities based on criteria such as:
  - Date / time
  - Camera
  - Alarm / event type
- Be capable of exporting digitally signed recordings (watermark)
- Allow for remote viewing and control of all functions
- Allow PTZ control, compatible with installed cameras
- Provide Network interface connection
- Provide alarm notification upon loss of video
- Support for H.264 video format (NVR only)

2.3.2 Video Analytics

Video Analytics must:

- Integrate with ACS. We request you to offer Kiwi
- Detect behavior patterns for motion and non-motion corresponding to highly configurable rules
- Allow multiple rules to be applied to a single camera
- Provide advanced detection such as:
  - Facial Recognition
  - Direction (for wrong-way detection)
  - Speed
  - Size
  - Classification of moving object
  - Unattended objects
  - Stopped vehicles
  - Human behavior detection for mass crowd management
  - People/ object counting
  - Tailgating detection
  - Loitering detection
  - Crowd detection
  - Object removal (theft)
  - Motion detection on PTZ presets
  - Be capable of filtering out natural disturbances such as:
    - Weather related conditions
    - Changing light conditions

2.3.3 Cameras

Minimum technical requirements for proper camera and lens selection are driven by the camera's purpose, desired resolution, and environmental considerations. The ultimate question is; does the camera deliver usable video as defined by its task and purpose?

The following is provided as general guidance:

- All cameras must be field located on the projected location
- General IP (fixed & PTZ) Cameras must:
  - Be color (day and night use if required for task and purpose) Have lens to support camera task and purpose. Variable focal length (vari-focal) lens should be installed. Auto iris lenses must be installed for outdoor use or any applications with varying light conditions
  - Be capable of multiple H.264 streams
  - Be capable of Power Over Ethernet (POE)
  - Have low light sensitivity to meet required task and purpose
  - Support multi-level security access and restrictions
- IR Illuminators must support the camera(s) task and purpose

2.3.4 Camera Housings / Domes

Camera and housing must be suitable for use in the environment in which it must be placed and support camera task and purpose.

Exterior enclosures provided with exterior dome cameras must include surge and lightning protection.

Please allow for the correct mounting hardware on poles, walls, etc.

2.3.5 Camera Power Supplies

Power supplies must be sized and sourced based on the specific project requirements and according to the manufacturer's specifications

All external and internal camera power supplies must be located in an appropriate enclosure as required by local code(s) and environment

Should be connected to emergency power, if available, to continue operation upon loss of primary electrical power

Allow for Power over Ethernet switches or injectors where possible

Allow for sufficient (PoE) current to PTZ cameras and External cameras which have heaters

Any suggestions over and above the current design are welcome.
Basic system cabling will be delivered and installed by others.

2.4 PSIM System

Further details can be found in **Appendix D: Annex D.8_Global Physical Security Technical Standards**

The vendor is to offer an Advancis Winguard system and its implementation, interfacing the intrusion, access, cctv and intercom system with each other

All relevant elements and licenses need to be included in the vendor proposal.

2.5 Commission, handover, training and as build documentation

Vendors need to include allowance in their bid to test and commission the system in liaison with Zalando Security and SIG allowing for 2 full days; provide handover and training for 2 full days at Zalando security personnel and provide digital as build documentation within 1 month after system completion

3.0 Scope Drawings

The following drawings are appended to this document to provide indicative information for the intended design:

Drawing Ref:
GF 6 Verona 24-10-2018 V2 multilayout
GF 6 Verona 24-10-2018 V2-Verona Entrance's
GF 6 Verona 24-10-2018 V2-Verona Mezzanine MPT
GF 6 Verona 24-10-2018 V2-Verona Office Cam
GF 6 Verona 24-10-2018 V2-Verona Office CR
GF 6 Verona 24-10-2018 V2-Verona Office MPT
GF 6 Verona 24-10-2018 V2-Verona Site_Plan CAM
GF 6 Verona 24-10-2018 V2-Verona Warehouse A+B+C+D CAM
GF 6 Verona 24-10-2018 V2-Verona Warehouse A+B+C+D CR
GF 6 Verona 24-10-2018 V2-Verona Warehouse A+B+C+D MPT