Ascendi's approach to Cybersecurity

May 2017

Index

02/ Ascendi's Overview

01/ Ascendi's Overview

ASCENDI acts in road infrastructure asset management, O&M business and toll collection services

Around **$2.6 Billion** global investment

Over 750 km under operation

Equity stakes in **5 Road Concessions**
2 more concessions under acquisition

01/ Ascendi's Overview

Significant experience and know-how in toll collection

AET (MLFF)

Toll collection systems enabling traffic free flow

6 contracts under operation (130 tolling points)

Traditional Toll Collection

Open or closed systems, manual and electronic

2 contracts under operation
(134 Manual lanes
83 electronic single lanes free flow)

01/ Ascendi's Overview

Facts and Figures

\ **700K** Transactions processed daily

\ **1.7M** customer accounts managed

\ More than **160 users** of the systems

\ Transaction mode: **78%** ETC, **13%** VTC, **9%** Manual

\ > **500K** images per day

\ **5.2M km** (aggregate distance travelled by all users) charged per day

\ Invoices/notices: **42.5k** processed per week

02/ Security framework

02/ Security framework

European Standards

\ EN 15509 – **Electronic Fee Collection** – Interoperability Application for DSCR

\ Security features and mechanisms based on the **general security framework** defined in EN 14906

\ **Image Security**: attribute adaptations according to CEN/TS 16439 (EFC - Security Framework)

Network Security Protocols

\ Network Architecture: **segmentation** and **protection**

\ Public Key Infrastructure (PKI), FTPS, HTTPS for webmail, SSL VPN, Ipsec Tunnel Private-to-private Network

Physical Security

\ **Monitored** datacenters (heat, fire, power, air conditioning, surveillance)

\ **Restricted** physical Access

02/ Security framework

Organization

\ Security **policies** and **procedures**

\ **Skilled** Technical **resources**

\ **Non-disclosure agreement** concerning personal, proprietary information and good practices using IT systems

Systems

\ **Security-by-design**

\ **Identity** and access Management

\ Environment **Segregation**

\ Penetration **Tests**

Business Continuity

\ Secure infraestruture - **virtualization** and high availability for Core Systems

\ **Centralized** enterprise **backup** and recovery, disaster **recovery** and endpoint data protection

\ **Disaster Recovery** OBO and CBO

\ **Business Continuity** Plan

02/ Security framework

Endpoint protection

Internet Access

\ Access controlled through the use of **white-lists**

\ Internet **access** only allowed **via proxy**

\ **Active Directory user groups** determine the Internet access

Email

\ **Email** is only allowed **internally** for Manual Toll-Operator team

\ All client interaction teams use an **unified account** (mono account per channel)

\ **Traceability**
All email sent to Clients by the unified accounts is duplicated to a read-only mailbox

Workstations \ Mobile Devices

\ **Predefined** software **images** for workstations

\ **Standard GPO** enforced restrictions on USB drives and other media

\ **Locked down baseline** according to Center for Internet Security benchmarks

\ Firewall rules **restrict access** to local addresses only (http proxy is local)

\ **Software update** via SCCM (critical security, antivirus and malware)

03/ Transactions and data access

03/ Transactions and data access

Access Profiles are defined per application module

Designação	Responsável	Operador Gestão Documental	Supervisor Gestão Documental	Operador VTC	Supervisor VTC	Operador CAP	Supervisor CAP	Operador CAT	S
Descrição	Responsável	Operador de Gestão Documental	Supervisão de Gestão Documental	Operador de Validação Manual de Fotografias e Quality Assurance	Supervisão de Validação Manual de Fotografias e Quality Assurance	Operador de Centro de Atendimento Presencial	Supervisão de Centro de Atendimento Presencial	Operador de Centro de Atendimento Telefónico	
SIGA	x	x	x	x	x	x	x	x	
Sistema de Gestão Documental (SGD) | Supervisor	x		x						
Sistema de Gestão Documental (SGD) | Operador GDOC	x	x							
Sistema de Gestão Documental (SGD) | Utilizador	x			x	x	x	x	x	
Toolkit	x	x	x	x	x	x	x	x	
Foto V	x			x	x				
Armis VVF | Operador	x			x					
Armis VVF | Supervisor	x				x				
OBO Ascendi | Operador	x			x					
OBO Ascendi | Supervisor	x				x				
OBO Qfree | Operador	x			x					
OBO Qfree | Supervisor	x				x				
Gestão de Vídeo-Verificações	x			x	x				
Gestão da Gravação de Aferições	x			x	x				
Taxas Erro dos Contadores	x			x	x				
SICOP | Easytool	x			x	x				
SAP CRM | Pivot	x		x						
SAP CRM | Operador - 1ª Linha	x								
SAP CRM | Operador - 2ª e 3ª Linha	x								
SAP Produtivo | SP01	x								
SAP Produtivo | ZVV_RIMPFAT	x								
SAP Produtivo | VA01	x					x	x		
SAP Produtivo | FB01	x								
SAP Produtivo | VF01	x								
SAP Produtivo | VF03	x								
SAP Produtivo | F-32	x								
SAP Produtivo | F-28	x								
SAP Produtivo | ZSD_VIAVERDE	x								
SAP Produtivo | ZVV_STOCK	x								
SAP Produtivo | ZVV_CAIXAIDS	x								
SAP Produtivo | ZVV_REPORTS	x								
SAP CBO | ZCBO_EDR	x								

Permission Matrix

- By system
- Read Only / Read & Write

03/ Transactions and data access

Access Profiles are defined per application module

Segregated by Area of responsibility

\ Overall containment of information access

\ Rigid boundaries

\ Team defined access

Segregation by function

\ Different degrees of access inside the boundaries

\ Almost atomic granularity of permissions

Assure the principle of the least privilege in information access

04/ External requests for information

04/ External requests for information

Requests for Information

By Clients

Client requests

\ Client must show personal identification and vehicles documentation

\ Data is verified with historic ownership data

Available information

\ Non paid transactions

- Travel information
- Photographic evidence – license plate ONLY

04/ External requests for information

Requests for Information

By Public Authorities

Request by legal enforcement Entities

\ Requires criminal proceeding (not civil)

\ Requires an associated court order

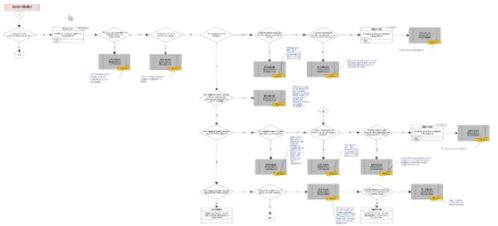
Available information

\ Non paid transactions

- Travel information
- Photographic evidence – license plate ONLY


S. R.
MINISTÉRIO DA ADMINISTRAÇÃO INTERNA
GUARDA NACIONAL REPUBLICANA
COMANDO TERRITORIAL DE COIMBRA
DESTACAMENTO DE TRÂNSITO DE COIMBRA
Ofício n.º 1
Proc. 3995 /MR-6F/09
Data :08-05-2009
ASSUNTO: Identificação de Condutor
Com os melhores cumprimentos
O Comandante de Destacamento


Tribunal Judicial de Cantanhede
2º Juízo
Rua dos Bombeiros Voluntários - 3060-163 Cantanhede
Telef: 231093500 Fax: 231093529 Mail: cantanhede.tc@tribunais.org.pt



05/ Next steps and challenges

05/ Next steps

- Address new data protection regulation
- **Security Audits**
- Perimeter reinforcement
- **Revise polices, procedures and rules**
- Evaluate CERT Team

05/ Challenges

- Digital Transformation
- Security awareness
- Involving suppliers and providers
- Attract Skilled resources
- Smart Cities, IOT, Mobility, New Payment Models


Thank You!
Questions ?
www.ascendi.pt
ascendi
ASECAP DAYS
PARIS 2017