TLN WRO Document

Wholesale Alternative Operator Security Policy

2/12/2014

Document Category and type

CAT	TYPE	DOC ID
Miscellaneous	**General**	**TLN_WRO_GA_G_M_PAAH**

Document Status

EDITION	DATE	STATUS
V 1.0	**2/12/2014**	**Final**

Legal Disclaimer

"This document constitutes an integral part of the Telenet Reference Offer for Basic TV / IDTV / BB and should be fully complied with by the Beneficiary at all times. Non compliance, incomplete or deviating application of this document by the Beneficiary, or his authorized agent, results in the suspension and ultimately termination of the Contract between Telenet and the Beneficiary.

At any time this document is susceptible to change by Telenet, Regulator's decision or by decision of a relevant judicial authority. Changes to this document will, depending on the circumstances for change, be appropriately notified to the Beneficiary and published on the Telenet website.

Telenet has appealed the CRC decisions of the VRM, BIPT and CSA of 1 July 2011 concerning the market analysis of the broadcasting market in Belgium and it consequently reserves all its rights in relation to this document."

1. INTRODUCTION

1.1 PURPOSE OF THIS DOCUMENT

The document intends to outline the information security requirements expected from the alternative operator who will use Telenet's wholesale offer. It is an inherent part of the Contract between Telenet and the Alternative Operator, later also referred to as AO.

1.2 SCOPE

The scope of the document is limited to the integration of the wholesale services offered by Telenet into the alternative operator's infrastructure as well as the processes that surround the use of these services.

1.3 AUDIENCE

The intended readers include people from both the administrative/legal area as well as security and technical personnel.

2. INTERFACE SET-UP AND SECURITY IMPLICATIONS

The wholesale offering has been set up in such a way, that AO personnel does not have direct access to Telenet's systems. All functionality required is offered through a secure API, which is linked to one specific AO. Per AO, a key is foreseen which is combined with the request, effectively making sure that the Chinese wall principle is implemented in each API call.

Following is an overview of all interfaces between Telenet and the AO. Per interface, the applicable security implications/requirements are listed. This document does not provide technical details on how the interface should be set up. Please refer to the appropriate technical project documentation for this information.

Each AO who applies for at least one RO of Telenet implies acceptance of the security requirements as outlined in this document.

2.1 APPLICATION PROGRAMMING INTERFACE (API)

This is the main interface through which all of the required functionality is offered. A standard web service endpoint is foreseen, using SOAP 1.1. The services are defined in 2 WSDL's, one covering order and product related functionality, the other covering functionality related to install and repair appointments, ticketing and CPE activation.

The AO will need to have an application in place which will call the required services through the API foreseen by Telenet.

- Per AO, a specific API is exposed. HTTPS, mutual authentication is foreseen so that both client as server side certificates are verified. The calling party has the responsibility to request a client certificate with a recognized Certificate Authority. After having received the certificate it needs to be sent to Telenet who can then register it to enable access. The calling party has the responsibility to check the validity of Telenet's server certificate associated with the web service endpoint. Details about this set-up must be kept secret by the AO and must not be shared with any other provider, subcontractor or partner.

- This API may not be called from any other location besides the location(s) as agreed upon by Telenet. In case additional AO affiliates require access, this must be discussed and agreed upon by Telenet, so that this may be set up properly.

- A unique key, assigned to the AO is linked to each service request entering Telenet's systems through this AO API. This key is automatically assigned by Telenet and enables the implementation of the Chinese wall and non-repudiation principle, separating calls from various AO's from one another.

- As no AO user ids will be defined on the Telenet systems, it is the obligation of the AO to foresee in proper user, authorization and log management linked to using Telenet's Wholesale services.
    - Which AO user has access to the AO application calling the Telenet Wholesale API services is left to the discretion of the AO. Full responsibility to set this up lies with the AO;
    - Which functions/services these users are able to use is left to the discretion of the AO. Full responsibility to set this up lies with the AO;
    - If the AO wishes to log user activity, the responsibility to set this up lies with the AO. This also includes any legal requirements that may be applicable when monitoring users, such as CAO81.
- Functionality for the AO Field Technicians will also be offered by the northbound API, which implies that communication with the field terminals will have to go through a proxy at the AO, and then access the API exposed to the AO.

3. GENERAL SECURITY REQUIREMENTS

This section outlines general security requirements which surpass the specific interface related requirements.

3.1 USE OF INFORMATION SYSTEMS

It is forbidden to hack into systems or in any other way circumvent the security measures installed to protect the system and the information it handles from unauthorised use, disclosure, modification, deletion, interruption or destruction. The Telenet systems to which the AO receives access are solely to be used in the light of the proper execution of the wholesale agreement between AO and Telenet.

The production systems are not intended for testing, and it is the AO's responsibility to train its agents in the proper use of the systems.

3.2 USE AND STORAGE OF AO END-CUSTOMER DATA

No AO end-customer data is kept in Telenet systems. In case technical interventions by Telenet technicians are required, a limited set of data enough to perform the intervention will be required. This data is treated as transaction data and is stored in a ticketing and workforce management system.

3.3 IDENTITY AND ACCESS MANAGEMENT

The AO is expected to have proper identity and access management systems and/or procedures in place to make sure access provided to AO personnel or contractors are kept up-

to-date and removed accordingly when leaving the company or changing functions within the company. Telenet is not in any way liable for damages inflicted on the AO because of improper user and access management by the AO.

3.4 SECURITY INCIDENT HANDLING AND NOTIFICATION

- In case the AO experiences a security incident which may affect Telenet's wholesale environment, the AO has the obligation to inform Telenet as soon as possible so that necessary steps can be taken to limit possible damage. In return, Telenet will also inform the AO in case it experiences security incidents which may affect the wholesale operations impacting the AO. For the sake of avoiding misinterpretations, a security incident is defined as follows:

  A security incident is a computer, network, or paper based activity which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data. It also includes threats, misrepresentations of identity, or harassment of or by individuals using these resources. Examples include, but are not limited to:

  - *(Distributed) Denial of Service attacks;*
  - *Hacking attempts to gain unauthorized access to a network, a system, an application or data;*
  - *Contamination by malware, including viruses, Trojan horses, worms, etc.*
  - *Laptop or mobile device theft where the laptop contains sensitive information (belonging to Telenet or the AO) or can easily be used to gain access to the network;*
  - *Spam and mail forgery that originates or is relayed through the AO's or Telenet's domains ;*
  - *Compromise of privileged accounts on computer systems;*
  - *Compromise of individual user accounts or desktop systems;*
  - *Disclosure of protected data, including paper disclosure, e-mail release or inadvertant posting of data on a web site;*

  Telenet must be notified when the security incidents occurring at the AO may jeopardize Telenet's systems, e.g. viruses may spread into Telenet's network, data may be stolen when the AO has been hacked, etc . Likewise, Telenet will inform the AO if a similar incident may impact the AO's operations.
- If you learn of security flaws (ineffective security, software errors or bugs, etc), this must be reported to Telenet, so that the problem may be fixed / followed up properly.

3.5 DEFINE AND EXCHANGE SECURITY CONTACT INFORMATION

- During the onboarding project, appropriate security related contact information will be defined and exchanged so that it becomes clear how and when people may be informed about security governance as well as operational security issues.

3.6 GENERAL SYSTEMS AND APPLICATION SECURITY

All systems and applications used to access or use Telenet's Wholesale service need to comply with the following high-level security requirements:

3.6.1 NETWORK CONNECTIVITY AND SECURITY

- Remote connection from the vendor's premises or elsewhere with the Telenet network can only be established using a Telenet installed or approved network connection. This is to be established during the AO on-boarding project. Changes to the involved network components after initial installation, must be requested to and approved by Telenet.

- The internal IT infrastructure of the AO must be separated from the external network connectivity to any untrusted network (including the Internet) by a well configured and tested firewall. When services are accessible from an untrusted network, a DMZ set-up has to be used.

- In case the AO provides external connectivity into its IT infrastructure to its employees, it must be secured using encryption (SSL, VPN) and proper authentication, preferably two factor authentication.

- In case the AO has connections to other customer or partner networks, it must be ensured that the connections are physically or logically separate from the connections used for Telenet, so that other customers or partners cannot get access to systems or information offered by Telenet.

3.6.2 PHYSICAL SECURITY

- The vendor's premises must be adequately secured so that unauthorized people cannot get access to the office area and computer area undetected.

- Any networking and/or server equipment connecting to Telenet's network or containing Telenet information must be physically protected and located in a data center or dataroom, with the following security requirements:

    - Access control system providing access to people with a strict need to enter the area;
    - HVAC;
    - Fire detection and extinguishing equipment (following applicable regulations for computer equipment);

3.6.3 VULNERABILITY / PATCH MANAGEMENT.

There must be a process in place to follow up on security vulnerabilities reported by the manufacturer of any product that is used to access Telenet's Wholesale services, so that vulnerabilities may not be exploited and access to Telenet's systems may become possible.

3.6.4 ANTI-VIRUS

- All ICT equipment running operating systems which are susceptible to virus attacks and other forms of malware, must be protected by an anti-virus product.
- The anti-virus software must be kept up to date as well as the virus signature files, which should be updated as soon as or shortly after the update becomes available.

3.6.5 TELENET INFORMATION PROTECTION.

The AO has to take reasonable precautions to make sure any Telenet information which may be located on its ICT systems is protected against unauthorised disclosure, modification, interruption or destruction, when stored and/or transmitted across the network.