TrustedX - Encryption Key Management

Whitepaper

CONTENTS

Introduction

Organizations are increasingly relying on encryption to protect application data. The growth in the use of this technology is occurring because of:

- **An increased data risk exposure** owing to factors such as the progressive externalization of the centers in which the data is stored.
- **The need to comply with data protection confidentiality regulations.**

Protecting data with symmetric keys requires solving how to manage and protect the keys used. For example:

- If an encryption key is lost, any data encrypted with it that cannot be recovered in cleartext will be unusable.
- When there is no adequate access control to the encryption keys, the key may be copied, which means that the encrypted data is left unprotected, regardless of the strength of the cryptographic algorithms used.

Encrypting and Managing Symmetric Keys with TrustedX

TrustedX data protection entails data encryption and decryption and the centralized management of symmetric keys

There are two types of data encryption and decryption:

- **Symmetric:** Data is encrypted and decrypted with a secret key.
- **Asymmetric:** Data is encrypted with a secret key that is, in turn, encrypted with the public keys of one or more recipients (digital envelope). This means that recipients decrypt the data by first decrypting the secret key with their public keys.

Symmetric key management therefore entails generating and storing the keys (custody) and retrieving them when the encrypted data needs to be accessed.

The main value of TrustedX resides in the fact that it allows you to perform all of these operations centrally, which makes it a data protection solution that applications can use as SOAP/WS and REST/WS services.

Centralizing these operations and making them accessible as security services has the following advantages:

- **It provides dynamic (role-based) access control for the data encrypted symmetrically by the organization's different systems.** By centralizing the storage and recovery of the symmetric keys used in the encryption operations, the systems that perform these operations are freed of having to distribute the keys to all the recipients authorized to read the data. All they have to do is use the storage (custody) operation. From this moment on, the symmetric key management service controls key access

based on the user's role in the organization. Consequently, any user that wants to retrieve the keys must prove that they have an identity that has been assigned the required role.

- **It allows governing the symmetric key management and all the data encryption and decryption processes.** Centralization allows applying corporate policies that regulate how these processes are performed. For instance, you can define the type of key used to protect the stored symmetric keys. You can also define the encryption algorithm for protecting the data depending on the degree of confidentiality allocated to the data with security labels.
- **It allows auditing the symmetric key management and the data encryption and decryption.** Centralization means that the events corresponding to the generation, custody and retrieval of symmetric keys along with those corresponding to the data encryption and decryption operations are all logged. This allows monitoring these operations and supervising what the organization uses them for in an effective manner.

CHAPTER 1

Encryption Key Management

TrustedX provides a platform for protecting data and managing encryption keys as either a physical (hardware) or virtual (software) appliance. It has a graphical administration console and a shell for managing the configuration of the entire system.

This platform contains the following elements:

- Encryption and Decryption service
- Symmetric Key Management Service

The functions offered by these services can be invoked from an application using the Web interfaces provided by the platform (SOAP/WS, REST/WS) or via a Java API.

The symmetric key management service can be accessed transparently from the user's desktop with Safelayer's KeyOne Desktop data encryption application.

Authentication and Authorization

All TrustedX's services are access-control protected (authentication and authorization), for which TrustedX uses the authentication and authorization service that is incorporated into the platform.

You define the accepted authentication mechanisms in the graphical administration console. Use of these mechanisms generally falls into the following scenarios:

- **The validation of the credentials is performed by TrustedX's authentication and authorization services** (e.g., username and password, client certificates received in TLS/SSL connections established directly with TrustedX).
- **The authentication and authorization service receives unvalidated credentials and delegates their validation to an external authentication validator (RADIUS, LDAP, Active Directory).** An example of this case is authentication in TrustedX through the validation of one-time passwords (OTP) by accessing a RADIUS authentication server.
- **Prior total or partial credential validation is performed by an external authentication agent.** The agent provides the identity of the client to the authentication and authorization service (total validation), or it provides the credentials to the authentication and authorization service, which then completes the validation (partial validation).

Encryption and Decryption service

The data encryption and decryption service centrally encrypts and decrypts data (on the server).

The messages exchanged with the service have a deliberately flexible structure that varies depending on the format chosen for representing the encrypted data or the data that you want to extract for decryption. The following service access profiles are supported:

- **CMS/PKCS#7 profile:** for encrypting any data and encapsulating it in an EnvelopedData (if the encryption is asymmetric) or EncryptedData (if the encryption is symmetric) type CMS/PKCS#7 structure. It also supports decrypting data encapsulated in any of these types of CMS/PKCS#7 structure.
- **XML-Enc profile:** for encrypting data in XML format and representing the result also in XML, encapsulating it in an <EncryptedData> element as defined in [XML-Enc]. It also supports retrieving, in cleartext, the data in XML format that the <EncryptedData> element encapsulates. It supports symmetric and asymmetric encryption.
- **S/MIME profile:** for encrypting a MIME entity (e.g., an email message) and encapsulating it in another that is returned as the result. The original MIME entity is first encapsulated in an EnvelopedData type CMS (S/MIME v3) or PKCS #7 (S/MIME v2) structure, which is then represented in S/MIME format, i.e., it is encoded in base64 and put in the body of a MIME entity that has the following fields in its header:

  Content-Type: application/pkcs7-mime; smime-type=enveloped-data.
  Content-Transfer-Encoding: base64

  It also supports retrieving, in cleartext, a MIME entity encrypted in the body of another that encapsulates it.
- **WS-Security profile:** for encrypting any element of a SOAP message (or its content) and returning, as the result, a SOAP message complying with the [WSS] specification. The encrypted element (or content) is encapsulated in an <EncryptedData> element in the returned SOAP message. In addition, the <Security> header of this message includes an <EncryptedKey> element that contains the symmetric key used for the encryption, which is in turn protected by the public key of the message recipient. It also supports retrieving, in cleartext, a SOAP message that has one or more of its elements (or the content of these elements) encrypted and, therefore, encapsulated (each of them) in the corresponding <EncryptedData> element.

Symmetric Key Management Service

The symmetric key management (SKM) service centrally generates, stores (custody) and retrieves symmetric keys.

The keys are managed in accordance with the criteria defined in a given policy. For example:

- What type of key is to be used to protect the keys in custody.
- Whether the custody keys must be stored in an HSM.
- Whether an HSM must be used for generating symmetric keys.

Entities (users, applications) use this service to encrypt a document with a symmetric key and send it to the symmetric key management service, which protects the key and only provides it to users that are part of a defined trust circle. This provides the following advantages:

- The entity is not responsible for protecting the encryption key. TrustedX carries out this task.
- The entity does not have to worry about sending the encryption key to the document recipients. TrustedX manages who can retrieve the key for decrypting the document through its authentication and authorization service, which provides key access control based on group membership.

The symmetric encryption keys can be generated by an external application or by the TrustedX platform.

KeyOne Desktop

KeyOne Desktop is a desktop application for performing cryptographic operations on the files in the file system. These operations appear as options in a contextual menu displayed when you right-click the cursor on a file.

KeyOne Desktop allows both symmetrically and asymmetrically encrypting files. For symmetric encryption, the encryption key can be generated by KeyOne Desktop or by TrustedX, depending on the configuration of KeyOne Desktop.

In all cases, KeyOne Desktop requests that TrustedX protects the key to be used and is returned an identifier for retrieving the key for performing decryptions.

The identifier is stored in a CMS structure that KeyOne Desktop uses to encode the encrypted data. So, when the user requests the decryption operation, KeyOne Desktop obtains the corresponding key identifier and requests the decryption key from TrustedX.

CAPÍTULO 1

Architecture and Operation

When applications want to encrypt or decrypt data, they access the operations of the platform's data encryption and decryption service (encrypt, decrypt). For performing asymmetric encryption operations, the recipients for whom the data is encrypted are specified in the access message sent by the applications to the service. Each of these recipients can subsequently retrieve the data in cleartext by requesting the decryption operation from the service. For performing symmetric encryption or decryption, the symmetric key to be used for the operation is specified in the access message sent by the applications to the service.

Symmetric key management supports generating (genKey), storing (putKey) and retrieving (getKey) symmetric keys. The protected keys are stored in a database (or other type of repository) encrypted with the key of a given symmetric key management policy (custody key), and each of them is associated to a resource registered in TrustedX. The custody key is saved in the keystore of the policy to which it belongs and is based, normally, on an HSM device (Figure 1-1).

Access to both the encryption and decryption service operations (encrypt, decrypt) and the symmetric key management operations (genkey, putkey, getkey) is controlled by TrustedX's authentication and authorization service (authn, authz). In the specific case of retrieving keys stored in custody, the authentication and authorization service checks both that users, according to their roles, have the permissions for executing the operation of the service (getKey) and also that they have access to the symmetric key that they want to retrieve.

The platform generates a detailed log with all the events that occur in it as a result of service consumption and configuration management. This log data can be stored in databases and syslog servers.

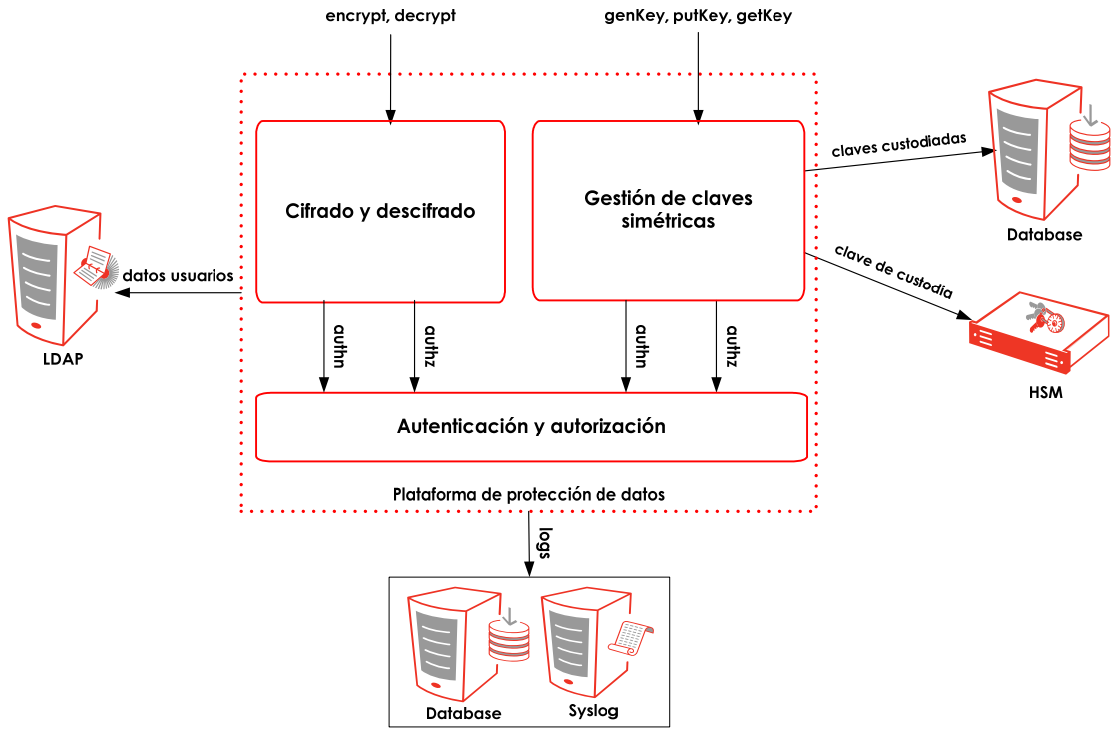

Figure 1-1. Encryption, decryption and symmetric key management.

CHAPTER 2

Administration

TrustedX administration comprises two clearly differentiated domains. On the one hand, there is the administration of the system configuration and the access to the log records generated by the services. On the other, there is the administration of the appliance, i.e., of the execution platform on which TrustedX operates:

- The first type of administration is done using a Web application that forms part of the system. It has a graphical interface in which you can manage the TrustedX configuration and browse the log records.
- The second type involves using an application called the command-line administration console (or the shell), which you access via the physical terminal of the appliance or from a remote terminal connected via SSH.

Graphical Administration Console

The graphical administration console is a Web application for administering and accessing all the information that TrustedX handles using a browser.

In terms of data encryption and decryption and symmetric key management, this application implements the following functions:

- **Management of end-entities:** for registering users, applications and services as end entities and administrating their data. It also supports defining groups of end entities.
- **Management of authentication and authorization policies:** for defining the authentication and authorization policies for controlling the access to the end entities of the TrustedX services.
- **Management of encryption and decryption policies:** for defining and making changes to the policies applied for encrypting and decrypting data.
- **Management of symmetric key management policies:** for defining and editing the policies applied for managing the stored symmetric keys (Figure 2-2).

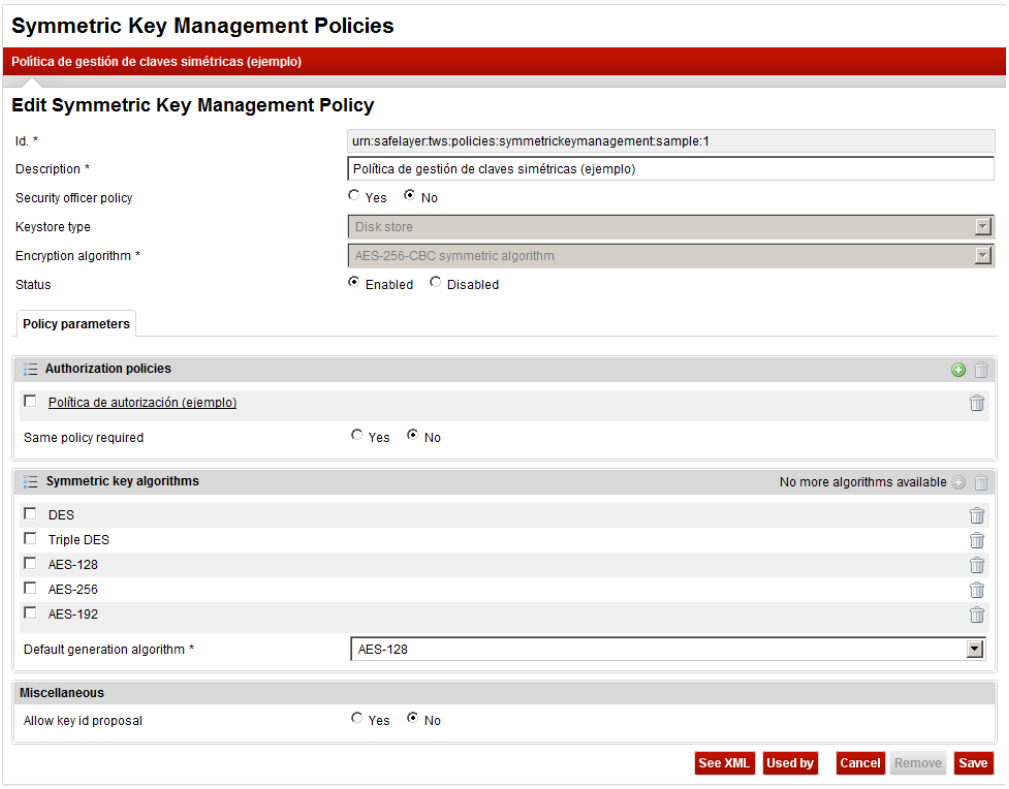

Figure 2-2. Management of symmetric key management policies.

- **Management of the configuration of the services:** for defining the configuration of the services in the platform.
- **Management of the configuration of the connections with the repositories:** for defining the configuration of the connections for accessing the different repositories (databases, LDAP services) used by the system.
- **Management of the access configuration for HSM devices:** for defining the configuration used for accessing the HSM devices used by the platform.
- **Log browsing and auditing:** for browsing the events generated by all the service components of the platform.

Command Shell

This application, which, as its name suggests, has a command-line user interface, is for administering the system on which TrustedX is run (Figure 23). You can use it to:

- Install the license file in the appliance's file system.
- Install the license file in the appliance's file system.
- Configure the appliance's network interface.
- Install the drivers and define the client configuration so TrustedX can access the elements that make up its operating environment (databases, HSM devices, etc.):

This application's commands are hierarchically organized in a multi-level structure. All the commands have a very similar syntax that can be checked using the help command. Pressing the 'tab' key autocompletes commands and displays their options.

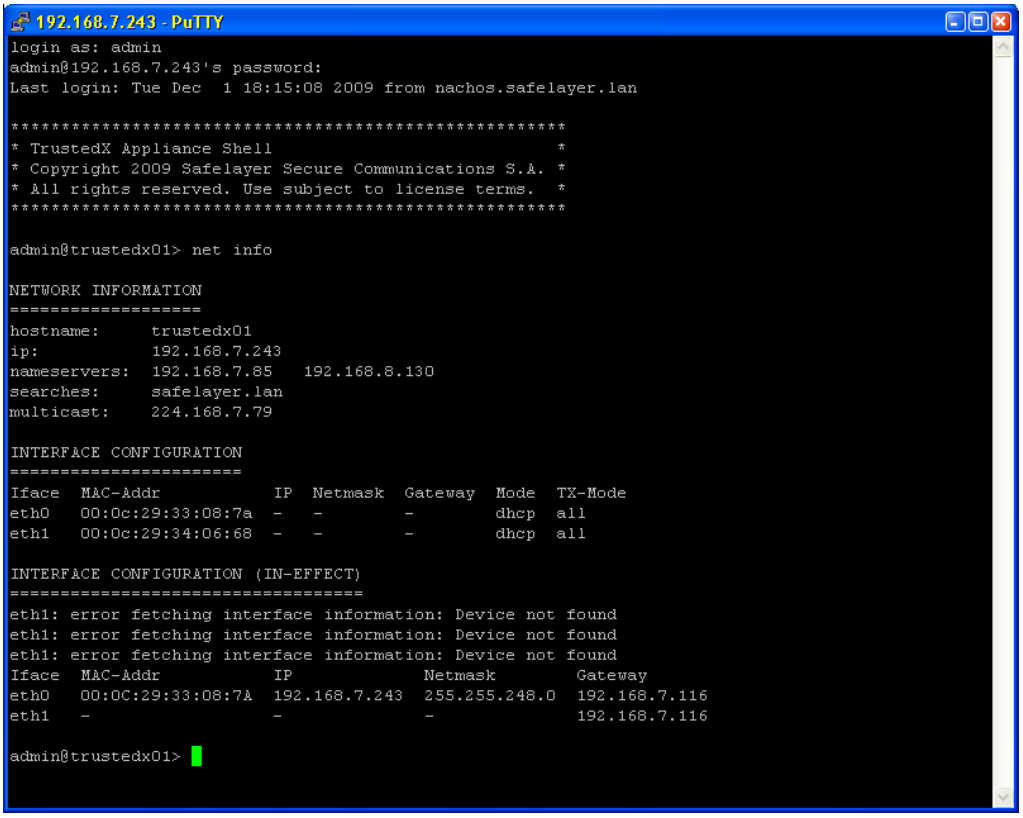

Figure 23. Command-line administration console.

High Availability

The TrustedX's services can be deployed in high availability so that they are always accessible. This deployment's architecture is illustrated in Figure 2-4.

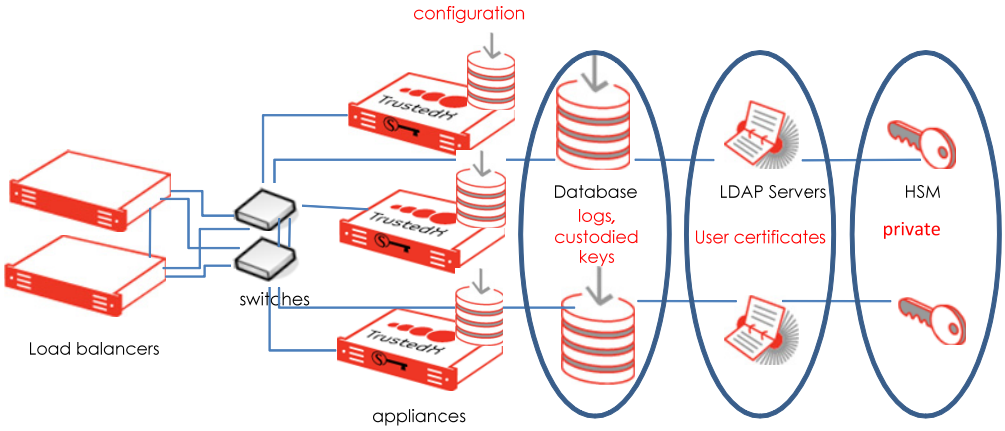

Figure 2-4. TrustedX high-availability deployment.

This architecture has a cluster formed by two or more TrustedX appliances to which a load balancer, also in high availability (e.g., active/passive configuration), distributes the requests received from clients. All the systems and resources (log databases, LDAP servers, HSM devices, etc.) that the TrustedX services access must be in high availability.

Monitoring and Auditing

Monitoring in TrustedX is carried out using a SNMP agent and aims to assure the correct operation of the platform (Figure 2-5). The organization's external monitoring product receives traps from this agent in real-time when an exceptional situation occurs.

In addition, the external monitoring product also sends requests to the SNMP agent (probing) to detect failures during periods of apparent inactivity. With the data obtained via the monitoring product, reports can be created for the organization's IT systems department.

Auditing is performed by sending all the activity that occurs in the platform to an external system (e.g., Splunk) using syslog (Figure 2-5) to generate business and compliance reports.

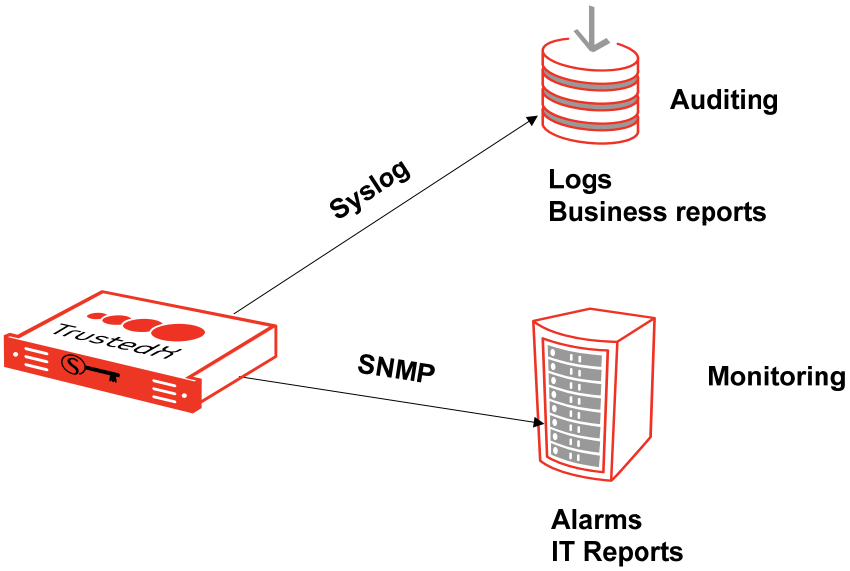

Figure 2-5. TrustedX monitoring and auditing.

APPENDIX A

Supported Encryption Standards and Algorithms

This appendix lists the encryption standards and algorithms supported by TrustedX.

Standards

TrustedX supports the following standards:

Reference	*Standard*
[CMS]	Cryptographic Message Syntax, IETF RFC 5652
[LDAP]	Lightweight Directory Access Protocol
[PKCS#7]	PKCS #7: Cryptographic Message Syntax, version 1.5. IETF RFC 2315
[SMIME2]	S/MIME Version 2 Message Specification, IETF RFC 2311
[SMIME3]	S/MIME Version 3 Message Specification, IETF RFC 2633
[SOAP]	Simple Object Access Protocol Version 1.1, W3C. May 2001
[SSL/TLS]	Secure Socket Layer / Transport Layer Security
[X509]	ITU-T Recommendation X509v3
[XML-Enc]	XML Encryption Syntax and Processing. W3C Recommendation 10 December 2002
[WSDL]	Web Service Description Language (WSDL) 1.1, W3C. March 2001
[WSS]	OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) February 2006

Encryption Algorithms

TrustedX supports the following encryption algorithms:

- RC2
- DES
- Triple DES
- AES-128

- AES-192
- AES-256
- RSA

© Copyright 1999-2013 Safelayer Secure Communications, S.A. All rights reserved.

TrustedX Encryption Key Management - Whitepaper

This document and the software described in it are supplied under license and may be used or copied only in accordance with the terms of the license. This document is for informational use only. Safelayer Secure Communications S.A. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. The content of this document is subject to change without notice.

The copyrighted software that accompanies this document is licensed to the end user for use only in strict accordance with the End User License Agreement, which the licensee should read carefully before using the software. Except where permitted by the license, no part of this document may be copied, reproduced or stored in any form or by any means, electronic or mechanical, by recording or in any other way, without the express permission of Safelayer Secure Communications, S.A.

TrustedX and KeyOne are Safelayer trademarks. All other names may be trademarks or registered trademarks of their respective owners.

Safelayer Secure Communications, S.A.

Telephone: +34 93 508 80 90

Fax: +34 93 508 80 91

Web: www.safelayer.com

Edificio Valrealty C/ Basauri, 17 Edifico B Pl. Baja Izq. Of. B 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: +34 91 3076652
World Trade Center (Edif. S-4), Moll de Barcelona S/N 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: +34 93 5088091