Document title

EURONEXT SECURE COMMUNICATIONS STANDARDS

Document type or subject

GENERAL OVERVIEW

Revision number	Date
Revision Number: 1.0	14 June 2022
Number of pages	Author
10	Euronext

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided "as is" without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, Euronext does not guarantee its accuracy or completeness. Euronext will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of financial products that are traded on the exchanges operated by Euronext's subsidiaries shall depend solely on the applicable rules of the market operator. All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext.

Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at www.euronext.com/terms-use.

PREFACE

PURPOSE

The purpose of this document is to provide information about the cryptographic controls (ciphers, encryptions and hashing algorithms) accepted by Euronext.

TARGET AUDIENCE

The target audience for this document are the Euronext customers that use Euronext Web Hosted Applications.

WHAT'S NEW?

The following lists only the most recent modification made to this version.

REVISION NO./ VERSION NO.	DATE	AUTHOR	CHANGE DESCRIPTION
1.0	14 June 2022	Euronext	Version 1

CONTENTS

1. INTRODUCTION

This document is intended to be read by Euronext customers to ensure that they can interact securely with multiple web-based Euronext applications and services. Data entered into web-based applications and service sessions must take place over HTTPS, using SSL/TLS to guarantee the communication's:

- confidentiality (through encryption)
- integrity (through message integrity checks i.e. MAC); and
- authenticity (through mutual authentication).

This security measure will provide an additional protection to all users of Euronext applications.

This document specifies the security standard for secure communications protocols used in Euronext Web Hosting applications.

1.1 SCOPE

The applications in scope are all the web hosting applications on Euronext infrastructure. These applications are accessed by customers and must have security standards enforced to maintain clients' protection.

The applications that must follow this standard are:

- EOD (End of Day)
- NDM (Non-Real-Time Data Management)
- PLUG (Product Listing Universal Gateway)
- PTRM (Post-trade Risk Management "RiskGuard")
- SCORE (System for Centralisation of Offers on Regulated and Unregulated Markets of Euronext)
- TCS (Trade Confirmation System)
- EFS (Euronext File Services)
- SATURN (APA/ARM/OBOE/SCL/CPR)
- EIM (Euronext Inventory Manager)
- Direct (previously ISE Direct)

The standard applies in both the EUA and Production environments.

1.2 WAIVERS AND EXCEPTIONS

All customers must be compliant with the technical details specified below. In the event of a customer not being compliant or not supporting the technical specifications defined in this document, they must take the appropriate steps to support them as soon as possible.

Customers that do not support or are not compliant with the specifications will be given a two-month period to implement the necessary changes.

During these two months, the customer can contact their Euronext point-of-contact and a solution will be provided for a temporary resumption of the service.

After the period of two months, Euronext will not guarantee further support of non-compliant usage of the Euronext Web Hosting applications.

2. SECURE COMMUNICATIONS PROTOCOLS

Secure communications take place when a conversation between two entities cannot be listened to by a third party. For this to be the case, the information must be transmitted in a way such that no unauthorised third party is able to read the data or tamper with it. A specific communication protocol must therefore be established between the two entities. This protocol will handle the cryptographic mechanisms and configurations necessary to ensure that the communication is indeed secure. The server should be authenticated by a certificate signed by a mutually recognised certification authority, that has not expired and has not been revoked.

To enable secure communications, HTTPS (Hypertext Transfer Protocol Secure) must be enforced for every communication. HTTPS is a variation of the normal web communications protocol (HTTP) that operates on top of Transport Layer Security (TLS), which is the successor to Secure Sockets Layer (SSL). TLS is more secure than SSL, since it has had had several modifications through the years aimed to strengthen the protocol – namely stronger cipher suites. It consists of a combination of authentication, encryption and message authentication code algorithms.

The algorithms used for secure communication should be chosen accordingly. There are versions of TLS with known vulnerabilities that can compromise the data while it is in transit. Besides this, using weak hashing algorithms results in the communication being less secure.

2.1 ACCEPTED PROTOCOLS

The following accepted protocols are advised to ensure compliance with this standard:

- HTTPS connections should enforce **TLSv1.2 or above**
- All HTTPS connections should be directed to the **443 TCP port** of the relevant application.

The following outdated/vulnerable protocols are **not** supported by Euronext:

- ✗ SSLv2
- ✗ SSLv3
- ✗ TLS1.0
- ✗ TLSv1.1

2.2 ACCEPTED CIPHER STRINGS

The following suite configuration (Table 1), designed for both RSA and ECDSA keys, are listed in order of preference for configuration (best key exchange algorithm/strongest encryption first).

TABLE 1: ACCEPTED CIPHER SUITES

Protocol	Key Exchange Algorithm	Authentication Algorithm	Bulk Encryption Algorithm	Mac Algorithm
TLS 1.3	Any	Any	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
TLS 1.3	Any	Any	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
TLS 1.3	Any	Any	ChaCha20 (CHACHA20)	SHA256
TLS 1.2	Elliptic Curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
TLS 1.2	Elliptic Curve Diffie–Hellman (ECDH)	RSA	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
TLS 1.2	Elliptic curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	ChaCha20 (CHACHA20)	POLY1305
TLS 1.2	Elliptic curve Diffie–Hellman (ECDH)	RSA	ChaCha20 (CHACHA20)	POLY1305
TLS 1.2	Elliptic Curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
TLS 1.2	Elliptic curve Diffie–Hellman (ECDH)	RSA	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
TLS 1.2	Diffie–Hellman (DH)	RSA	AES 256 (AES256 - GCM)	SHA384
TLS 1.2	Diffie–Hellman (DH)	RSA	AES 128 (AES128 - GCM)	SHA256

3. TROUBLESHOOTING GUIDE

To increase the effectiveness of troubleshooting any connection errors on Euronext Web hosting applications, please provide the following information to the Euronext support teams:

TABLE 2: TROUBLESHOOTING INFORMATION TO PROVIDE TO SUPPORT TEAMS

Information	Description	Runbook	Expected Output (Example)
Operating system	What operating system is running when the error occurs	For Linux: "**uname -a**" For windows: open CMD and write **winver**	*Linux x.x.0-xxx.el7.x86_64*
Java version	What is the Java version you are running (some older versions of Java may not support our standard)	Follow official java guide - here.	*java version "1.x.0_xx"* *Java(TM) SE Runtime Environment (build 1.7.0_55-b13)* *Java HotSpot(TM) 64-Bit Server VM (build 24.55-b03, mixed mode)*
.NET Framework version	What version of .NET is the application built upon	Follow official Microsoft guide – here.	*.NET Framework 4.5*
Open SSL	What is the OpenSSL version currently in use	Run command: "***openssl version***"	*OpenSSL 1.0.1e-fips 11 Feb 2013*
Curl version	What is the curl version currently in use	Run command: "**curl -V**"	*curl 7.29.0 (x86_64-redhat-linux-gnu) libcurl/7.29.0 NSS/3.16.2.3 Basic ECC zlib/1.2.7 libidn/1.28 libssh2/1.4.3* *Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtsp scp sftp smtp smtps telnet tftp* *Features: AsynchDNS GSS-Negotiate IDN IPv6 Largefile NTLM NTLM_WB SSL libz*
Browser version	What is the browser version currently in use	May vary from browser to browser. Information in found generally in the Help section (About).	*Google Chrome Version 75.0.3770.100 (Official Build) (64-bit)*

Curl request example	Simple connection test to identify certain handshake parameters (bold)	Run the command: **“curl - vvv <Euronext website>”**	* Initializing NSS with certpath: sql:/etc/pki/nssdb * CAfile: /etc/pki/tls/certs/ca-bundle.crt CApath: none * SSL connection using **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** * Server certificate: * subject: CN=efs.euronext.com,O=Euronext Technologies,L=Paris,C=FR * start date: May 04 09:18:31 2017 GMT * expire date: May 04 09:48:29 2020 GMT * common name: efs.euronext.com * issuer: CN=Entrust Certification Authority - L1K,OU="(c) 2012 Entrust, Inc. - for authorized use only",OU=See www.entrust.net/legal-terms,O="Entrust, Inc.",C=US

3.1 KNOWN CONNECTIVITY ISSUES

This section describes any known connectivity issues, to help Euronext customers diagnose and fix connectivity problems while accessing the Euronext web applications in the scope of this document.

TABLE 3: KNOWN CONNECTIVITY ISSUERS

Technology	Error	Mitigation
.NET Framework	*WebException occurred.* *Message is:* *The request was aborted: Could not create SSL/TLS secure channel.*	Add to the application code: *ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;*
Curl Connection (Linux)	*Curl: (35) SSL connect error*	Upgrade installed Curl package

4. CONTACTS

Operational Client Services Desk

Telephone:

Belgium	+32 2620 0585	Norway	+31 20 721 9585
France	+33 1 8514 8585	Portugal	+351 2 1060 8585
Ireland	+353 1 6174 289	UK	+44 207 660 8585
Netherlands	+31 20 721 9585		

Email: clientsupport@euronext.com

Service hours: 08:00 – 19:00 CET/CEST