ADACOM PUBLIC CERTIFICATION SERVICES
Relying Party Agreement for Class 1-3 Certificates

YOU MUST READ THIS RELYING PARTY AGREEMENT BEFORE VALIDATING AN ADACOM CLASS 1-3 CERTIFICATE (DIGITAL ID^{SM}) (HEREAFTER REFERRED TO AS "DIGITAL CERTIFICATE") OR OTHERWISE ACCESSING OR USING ADACOM's DATABASE OF DIGITAL CERTIFICATE REVOCATIONS AND OTHER INFORMATION (HEREAFTER REFERRED TO AS "REPOSITORY"). IF YOU DO NOT AGREE TO THE TERMS OF THIS RELYING PARTY AGREEMENT (HEREAFTER REFERRED TO AS "AGREEMENT"), YOU ARE NOT AUTHORIZED TO USE ADACOM'S REPOSITORY.

This Agreement becomes effective when you submit a query to search for a digital certificate, or to verify a digital signature created with a private key corresponding to a public key contained in a digital certificate, or when you otherwise use or rely upon any information or services provided by ADACOM's Repository or website relating to a digital certificate.

You acknowledge that you have access to sufficient information to ensure that you can make an informed decision as to the extent to which you will chose to rely on the information in a digital certificate. For more educational material, see the tutorial contained in ADACOM's repository at https://www.adacom.com/repository . YOU ARE RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A DIGITAL CERTIFICATE. You acknowledge and agree that your use of ADACOM's Repository and your reliance on any digital certificate shall be governed by ADACOM's applicable Certification Practice Statement (hereafter referred to as the "CPS") as amended from time to time, which is incorporated by reference into this Agreement. The applicable CPS is published on the Internet in the Repository at https://www.adacom.com/repository/CPS and is available via E-mail by sending a request to: CPS-requests@adacom.com . Amendments to the applicable CPS are also posted in ADACOM's Repository at https://www.adacom.com/repository/updates .

Additional Terms and Conditions: The digital certificate corresponding to the digital signature you are relying on was issued in accordance with the requirements set forth under the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and (hereafter referred to as "EU Directive") and the Greek Presidential Degree 150/2001 on the Adaptation of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (Government Gazette Issue No. 125/A'/25.06.2001). ADACOM S.A. is registered in the Certification Service Providers' Registry of the Hellenic Telecommunication and Post Commission as a Certification Service Provider issuing Qualified Certificates by its declaration
http://www.eett.gr/nopencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatur es/EsignProviders.html

The following table indicates how you know what the object identifier ("OID") and certificate policy (Class 1-3) corresponding to the digital certificate is.
ADACOM S.A.'s certificate policies are described in the document "VeriSign Trust Network Certificate Policies (VTN CP)". A copy of this document may be found at
https://www.adacom.com/repository/cp and at
http://www.verisign.com/repository/vtnCp.html

OID	VTN CP Terminology
VeriSign/pki/policies/vtn-cp/class1 (2.16.840.1.113733.1.7.23.1).	Class 1
VeriSign/pki/policies/vtn-cp/class2 (2.16.840.1.113733.1.7.23.2).	Class 2
VeriSign/pki/policies/vtn-cp/class3 (2.16.840.1.113733.1.7.23.3)	Class 3

As a result, the following terms shall also apply to you.

1. You shall verify the validity, suspension or revocation of the digital certificate using current revocation status information prior to relying on a digital signature created with a private key corresponding to a public key contained in a digital certificate. A method by which you may check Certificate status is by consulting the most recent Certificate Revocation List from the Certification Authority that issued the digital certificate on which you wish to rely.

2. You shall take account the specific limitations on the usage of the digital certificate indicated to the relying party in the applicable CPS. Generally:

- Digital Certificates shall be used only to the extent use is consistent with applicable law
- ADACOM S.A. digital certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.
- Class 1 client certificates are intended for client applications and shall not be used as server or organizational certificates, or as proof of identity or as support of nonrepudiation of identity or authority. In addition, Class 3 organizational certificates issued to devices are limited in function to web servers or web traffic management devices and/or object signing. Further, Administrator Certificates shall only be used to perform administrator functions. Certification Authority (CA) Certificates may not be used for any functions except CA functions.3. You shall take any other precautions prescribed in this Agreement.

AS EXPRESSLY PROVIDED IN THE CPS, ADACOM S.A. PROVIDES LIMITED WARRANTIED, DISCLAIMS ALL WARRANTIES AND OBLIGATIONS OF EVERY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF THE INFORMATION PROVIDED, AND FURTHER DISCLAIMS ANY AND ALL LIABILITY FOR NEGLIGENCE OR LACK OF REASONABLE CARE.

IN NO EVENT SHALL ADACOM S.A. BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER

INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, NONPERFORMANCE, OR UNAVAILABILITY OF DIGITAL CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED HEREIN, EVEN IF ADACOM S.A. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT WILL THE AGGREGATE LIABILITY OF ADACOM S.A. TO ALL PARTIES (INCLUDING YOU) EXCEED THE APPLICABLE LIABILITY CAP FOR SUCH QUALIFIED CERTIFICATE SET FORTHIN THE TABLE, BELOW.THE COMBINED AGGREGATE LIABILITY OF ADACOM S.A. TO ANY AND ALL PERSONS CONCERNING A SPECIFIC QUALIFIED CERTIFICATE SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED THE FOLLOWING, FOR THE AGGREGATE OF ALL DIGITAL SIGNATURES AND TRANSACTIONS RELATED TO SUCH DIGITAL CERTIFICATE:

Class of Certificate	Aggregate Liability
Class 1	100,00 Euros
Class 2	3.000,00 Euros
Class 3	75.000,00 Euros

YOU ARE HEREBY NOTIFIED OF THE POSSIBILITY OF THEFT OR OTHER FORM OF COMPROMISE OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A DIGITAL CERTIFICATE, WHICH MAY OR MAY NOT BE DETECTED, AND OF THE POSSIBILITY OF USE OF A STOLEN OR COMPROMISED KEY TO FORGE A DIGITAL SIGNATURE TO A DOCUMENT.

For information regarding private key protection, see
https://www.adacom.com/repository/PrivateKey_FAQ

Records related to the digital Ccrtificate application you are about to rely on, the relative Certification Authority's event logs, as well as the digital Certificate itself, will be security kept by ADACOM S.A. for the following terms:

- Additional five (5) years, after the revocation or expiration day of a Class 1 Certificate.
- Additional ten (10) years, after the revocation or expiration day of a Class 2 Certificate.
- Additional thirty (30) years, after the revocation or expiration day of a Class 3 Certificate.

If any provision of this Agreement, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this Agreement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

You agree that any disputes related to the services provided under this Agreement shall be governed in all respects by and construed in accordance with the laws of Greece, excluding its conflict of laws rules.

To the extent permitted by law, before you may invoke any dispute resolution mechanism with respect to a dispute involving any aspect of this Agreement, you shall notify ADACOM S.A. , and any other party to the dispute for the purpose of seeking dispute resolution. If the

dispute is not resolved within sixty (60) days after the initial notice, then a party may seek legal resolution. All parties agree that the courts of Athens Greece, shall have exclusive jurisdiction and venue for hearing and resolving any dispute regarding the interpretation and execution of this Agreement.

You demonstrate your knowledge and acceptance of the terms of this Agreement by submitting a query to search for, or to verify the revocation status of, a digital certificate or by otherwise using or relying upon any information or services provided by ADACOM's Repository or website relating to a digital certificate. If you do not agree, do not submit a query. By clicking the Accept button, you are bound by and agree to the terms of this Agreement, as though you had signed it by hand.