PKI Disclosure Statement

Universign CA Hardware

Universign

7, rue du Faubourg Poissonnière, 75009 Paris, France

VERSION : 2.6	DIFFUSION : PUBLIC	Effective date : 15/05/2019

Contents

This document is the PKI Disclosure Statement (PDS) of Universign, a member of the Universign Trust Network (UTN), for its CA *Universign CA Hardware*. This declaration is not a substitute for the Certification Policy (CP) of the UTN or for the Certification Practice Statement (CPS) of the CA. The CP of the UTN and the CPS of the CA *Universign CA Hardware* are available at the address https://www.universign.com/en/certifications/.

The PKI Disclosure Statement summarises the terms and conditions of the certification services offered by the CA *Universign CA Hardware*. It is intended for Certificate Subscribers, Certificate Officers and Relying Parties. In no way does it constitute a contract between the CA and the Subscriber or between the UTN and the Subscriber.

The UTN refers to Cryptolog International, a simplified joint-stock company with a capital of 735,963 euros, the registered office of which is at 7 rue du Faubourg poissonnière, 75009 Paris, registered in the Companies Register of Paris under the number 439 129 164.

1 Point of contact

Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

Requests to revoke Certificates can be sent via the online form available at the address:
https://app.universign.com/en/revocation/.

2 Type of Certificate, procedure for the validation and use of Certificates

The CA issues Certificates that enable identifying the Subscriber who uses them to create an electronic signature or seal.

The CA issues the following Certificates:

- electronic signature Certificates, the Subscribers of which are natural persons;
  - Certificates in compliance with [ETSI 319 411-2] level QCP-n, corresponding to OID 1.3.6.1.4.1.15819.5.1.3.1;

  - Certificates in compliance with [ETSI 319 411-1] level LCP, corresponding to OID 1.3.6.1.4.1.15819.5.1.3.3;
  - Certificates in compliance with [ETSI 319 411-2] level QCP-n-qscd, corresponding to OID 1.3.6.1.4.1.15819.5.1.3.6;

- electronic seal Certificates, the Subscribers of which are legal persons
  - Certificates in compliance with [ETSI 319 411-2] level QCP-1, corresponding to OID 1.3.6.1.4.1.15819.5.1.3.5;
  - Certificates in compliance with [ETSI 319 411-1] level LCP, corresponding to OID 1.3.6.1.4.1.15819.5.1.3.4;
  - Certificates in compliance with [ETSI 319 411-2] level QCP-1-qscd, corresponding to OID 1.3.6.1.4.1.15819.5.1.3.7;

The CA validates the information and supporting documents comprising the Certification request sent by the Subscriber. The identity verification of the future Subscriber occurs via a physical face-to-face meeting or a method known to be equivalent to the former for issuing Certificates in compliance with [ETSI 319 411-2] level QCP-l or QCP-n.

3 Limits of use of the Certificate

The CA cannot be held liable for any use of the Certificate that does not comply with the CP of UTN.

The Certificates are not designed, provided or combined with any authorisation to use them in any context other than those defined by the Certification Policy, i.e. as an electronic signature and/or an electronic seal.

The Certificates issued by the CA cannot be used as identity proof or as a means of electronic identification within the meaning of Regulation no. 910/2014 of the European Parliament and of the Council of 23 July 2014.

The CA is not responsible for evaluating the appropriate nature of use of a Certificate.

Additional limits of use may be defined by the Subscriber Agreement signed between the CA and the Subscriber or by the Relying Party Agreement.

The CA collects and processes personal data in accordance with the Data Protection Policy available at the address: https://www.universign.com/fr/politique-protection-donnees-personnelles/.

4 Obligations of Certificates Subscribers

The Subscriber acknowledges that it has all the necessary information before using its Certificate.

The Subscriber pledges to:

- provide a registration file with accurate information;
- immediately inform the CA if the information contained in the registration file and/or the Certificate is incorrect and/or modified;
- immediately inform the CA if the Certificate Officer is replaced, if applicable;
- where applicable, hold the intellectual property rights on the information transmitted in the registration file;
- use the Certificate only for the purposes authorised by the CP of the UTN, by the Relying Party Agreement and by the regulations applicable in general;
- comply with all the requirements defined by the CP of the UTN, and especially generate and use cryptographic keys in a device and with algorithms that comply with the CP;
- refrain from reverse-engineering or attempting to take control of the software tools used by the CA in the context of the certification service;
- ensure the security of its authentication means in order to prevent the use of the keypair by unauthorised third parties; it particularly pledges to take all measures necessary to guarantee the confidentiality of the keypair activation means and to implement all measures for keeping the keypair under the exclusive control of Authorised Persons, where applicable.

Additional obligations may be defined by the Subscriber Agreement signed between the CA and the Subscriber.

5 Obligations of Relying Parties

The Relying Parties are required to ensure the appropriate use of the information contained in the Certificates, especially by:

- verifying the consistency between their requirements and the conditions and limits of use of the Certificate defined by the Relying Party Agreement and by the CP of UTN;
- verifying whether the Certificate is compliant with legal, regulatory or normative requirements required for the desired use;
- verifying the status of the Certificate that they wish to use, as well as the validity of all Certificates of the chain of trust;
- using the appropriate software and hardware for verifying the validity of the signatures or seals associated with the Certificates;
- ensuring the conditions and limits of use of the electronic signatures or electronic seals associated with the Certificates.

6 Control of the Certificate status by Relying Parties

An information service provided by the CA enables:

- using the OCSP (Online Certificate Status Protocol) to verify the status of a Certificate;
- using the certificate revocation lists of the CA.

Under normal operation, it is available 24/7 pursuant to the conditions defined by the CP of the UTN.

The service allows obtaining information on the revocation of Certificates of levels QCP-1, QCP-n, QCP-1-qscd and QCP-n-qscd, even after their expiry. In case of the discontinuation of the CA 's activity, the obligations related to the provision of information on the Certificate status are transferred in accordance with the stipulations of the CP.

The Certificate revocation lists can be downloaded from the Publishing Site. The CRLs (Certificate Revocation Lists) are compliant with standard IETF RFC 5280.

The information required for using the OCSP protocol to verify the status of Certificates is contained in the Certificate fields and their extensions. The protocol is implemented as per standard IETF RFC 6960.

7 Limitations of guarantees and limitations of liabilities

Except for the guarantees expressly defined in the Relying Party Agreement applicable to the Relying Parties and those defined in the Subscriber Agreement applicable to the Subscriber, all other express or implicit guarantees are not applicable, especially any guarantee of suitability for a specific use or of compliance with special requirements of the Relying Parties and the Subscribers.

Therefore, the provision of the certification service does not discharge the Subscriber and the Relying Parties from analysing and verifying the legal or regulatory requirements applicable to it.

The CA cannot be held liable in case of an unauthorised or non-compliant use (with the legal and contractual requirements) of the Certificates, the revocation information as well as the equipment or software made available for the provision of the certification service.

The CA cannot be held liable for any damages resulting from errors or inaccuracies in the information contained in the Certificates, when these errors or inaccuracies result directly from the erroneous nature of the information communicated by the Subscriber. The CA cannot be held liable under any circumstance in case of any use that is not compliant with the uses defined in the CP or in the Relying Party Agreement. The CA cannot be held liable under any circumstance in case of breach of obligations by the Subscriber and/or the Relying Parties. The CA cannot be held liable for indirect damages resulting from the use of a Certificate.

Additional limitations may be defined by the Subscriber Agreement signed between the Subscriber and the CA.

8 Applicable documents

The applicable CP of the UTN, the Relying Party Agreement of the UTN and the CPS of the CA are published at the address http://docs.universign.eu.

9 Personal data protection policy

The Personal Data Protection Policy is published at the address: https://www.universign.com/fr/politique-protection-donnees-personnelles/

10 Reimbursement policy

The CA certification services are not subject to any reimbursement.

11 Applicable law

This declaration is governed by French law.

In case of a dispute arising from this declaration, the parties must first attempt mediation before bringing the matter before any court.

The mediation and arbitration centre of Paris shall be in charge of appointing a competent mediator. The matter may be brought before it by the first party to act and it then has a period of 6 months to accomplish its mission. The parties may decide to extend this period by mutual agreement. The matter may only be brought before a court after the expiry of this period, unless expressly agreed otherwise by both parties. They pledge to collaborate in good faith with the mediator. If the mediator is unable to gain both parties' consent, the first party to act may bring the matter before the court having jurisdiction in order to settle the dispute.

Consumers are informed that they have the option of appealing to a consumer ombudsman pursuant to the conditions defined in Title I of Book VI.

12 Audit of the certification authorities

The CA is regularly audited by an accredited body in accordance with standard EN 319 403 to ensure its compliance with the CP of UTN.