IDSCRIPT JURICERT® AUTHENTICATED TRUSTMINT® CERTIFICATE POLICY

1. INTRODUCTION

1.1 Overview

This Policy sets forth certain rules governing the issuance, management and use of IDscript Juricert Authenticated TrustMint Certificates ("IDscript Certificates").

Digital Signature Trust Co. ("DST"), as an independent contractor on behalf of IDscript Digital Credentials Inc. ("IDscript"), acts as Certification Authority in issuing, managing and revoking IDscript Certificates, as instructed and authorized by its IDscript, and provides Repository services with respect to such IDscript Certificates.

IDscript acts as Registration Authority (RA) in issuing, managing and revoking IDscript Certificates.

Juricert Services Inc. ("Juricert") provides Identification and Authentication ("I&A").

1.2 General Definitions

The following terms, when used in this Policy or related agreements, shall have the meanings indicated:

Certificate
A computer-based record or electronic message that: (a) identifies the Certification Authority issuing it; (b) names or identifies a Certificate Holder; (c) contains the Public Key of the Certificate Holder; (d) identifies the Certificate's operational period; and (e) is digitally signed by a Certification Authority. A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.

Certificate Holder
An Individual or Organization that: (a) is named or identified, or is responsible for the electronic device named or identified, in IDscript Certificate as the subject of such Certificate; and (b) holds the Private Key that corresponds to the Public Key listed in that IDscript Certificate.

Certificate Revocation List (CRL)
A database or other list of IDscript Certificates that have been revoked prior to the expiration of their validity period.

Certification Authority (CA)
An entity that creates, issues, manages and revokes Certificates.

Digital Signature
The transformation of an electronic record by one person using a Private Key and public key cryptography so that another person having the transformed record and the corresponding Public Key can accurately determine: (a) whether the transformation was created using the Private Key that corresponds to the Public Key; and (b) whether the record has been altered since the transformation was made.

Identification and Authentication (I&A)
To ascertain and confirm through appropriate inquiry and investigation the identity of a Certificate Holder, Relying Party or other entity, and to authenticate information contained in Certificate applications in conformity with the provisions of this Policy and related agreements.

IDscript Certificate
A Certificate issued pursuant to this Policy by DST as instructed to do so by IDscript.

Individual
A natural person, and not a juridical person or legal entity.

Key
A general term used throughout this Policy to encompass any one of the defined keys mentioned in this General Definitions section (e.g., Private Key and Public Key).

Key Pair
Two mathematically related Keys (a Private Key and its corresponding Public Key), having the properties that: (i) one Key can be used to encrypt a communication that can only be decrypted using the other Key; and (ii) even knowing one Key it is computationally infeasible to discover the other Key.

Organization
An entity that is legally recognized in the jurisdiction of its origin (e.g., a corporation, partnership, sole proprietorship, government department, non-government organization, university, trust, special interest group or non-profit corporation).

Policy
This IDscript Juricert Authenticated TrustMint Certificate Policy.

Private Key
The Key of a Key Pair kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.

Public Key
The Key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used to validate Digital Signatures created with the corresponding Private Key and to encrypt messages so that they can be decrypted only with the corresponding Private Key.

Registration Authority (RA)
An entity contractually delegated by IDscript to accept and process Certificate applications.

Relying Party
An individual or entity that has been authorized by IDscript, by contract or otherwise, to rely upon IDscript Certificates that have been issued pursuant to this Policy and at the direction of such IDscript.

Repository
An online system maintained by DST for storing and retrieving IDscript Certificates and other information relevant to IDscript Certificates and Digital Signatures, including information relating to certificate validity or revocation.

1.3 Identification

The Object Identifier ("OID") for this Policy, to be asserted in IDscript Certificates issued in accordance with this Policy, is: {joint-iso-ccitt (2) country (16) USA (840) US-company (1) DST (113839) CP (0) TrustMintExpress (5) IDscript Certificate (1)}.

1.4 Community and Applicability

IDscript determines and designates who is authorized to be a Registration Authority, Certificate Holder or Relying Party for the IDscript Certificates issued under this Policy.

1.5 Contact Details

Questions regarding this Policy should be directed to IDscript Digital Credentials Inc., Box 1107, Humboldt, SK S0K 2A0, Attn: Administration, admin@idscript.com.

2. GENERAL LEGAL PROVISIONS

2.1 Obligations

In issuing IDscript Certificates that reference this Policy, IDscript disclaims any and all responsibility for: (a) performing Identification and Authentication of applicants, and (b) verifying the accuracy of information submitted by applicants. IDscript makes no warranties or representations to applicants, Certificate Holders, Relying Parties or any other party that may rely on or use IDscript Certificates.

2.2 Liability

IDscript disclaims any and all liability for the information contained in Certificates issued under this Policy, including all claims for misappropriation of identity and intellectual property infringement.

2.3 Financial responsibility

IDscript will not be liable, in contract, tort or otherwise, to any applicant, Certificate Holder, Relying Party or any other party with respect to the application for or issuance, management or use of any IDscript Certificate.

2.4 Interpretation and Enforcement

The law of the Province of Saskatchewan shall govern the enforceability, construction, interpretation, and validity of this Policy, without regard to its conflicts of law principles.

2.5 Privacy and Data Protections

IDscript Certificates and CRLs, and personal or corporate information appearing on them and in public directories, are not considered confidential. Information contained on a single IDscript Certificate or related status information will not be considered confidential, when the information is used in accordance with the purposes of providing Certification Authority or Repository services and carrying out the provisions of this Policy. However, such information may not be used by any unauthorized party or for any unauthorized purpose (e.g., mass, unsolicited e-mailings, junk e-mail, spam, etc.), and any information pertaining to the management of IDscript Certificates, such as compilations of certificate information, shall be treated as proprietary.

3 IDENTIFICATION AND AUTHENTICATION

IDscript does not perform, and assumes no liability for, the Identification and Authentication of applicants, Certificate Holders of IDscript Certificates or Relying Parties. Any additional policies and procedures in this category are determined by agreement between the IDscript and Juricert.

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

DST, acting in its capacity as CA, will follow the practices and procedures outlined in the Certification Practices Statement with respect to issuance, management and revocation of IDscript Certificates, except as may be required by any applicable agreement between DST and IDscript, or as IDscript may otherwise direct. All other policies and procedures concerning the issuance, validity periods, management and revocation of IDscript Certificates are determined by agreement between the IDscript and DST.

5 CERTIFICATION AUTHORITY FACILITY AND MANAGEMENT CONTROLS

All policies and procedures concerning DST's and IDscript's physical, procedural, personnel and other operational standards are determined by agreement between the IDscript and DST.

6 TECHNICAL SECURITY CONTROLS

DST maintains a reliable system to ensure the security of its Private Keys. All policies and procedures concerning DST's and IDscript's technical security controls, including without limitations, Key generation, Key length, Key validity period, Private Key protection, and computer and network security, are determined by agreement between the IDscript and DST.

7 CERTIFICATE AND CRL PROFILES

All policies and procedures concerning IDscript Certificate profiles and CRL profiles are determined by agreement between the IDscript and DST.

8 SPECIFICATION ADMINISTRATION

8.1 Policy Changes.

IDscript may correct errors, update, modify or amend this Policy from time to time. IDscript will notify DST of any correction, updates, modifications or amendments in accordance with the agreements between DST and IDscript. Any suggested modifications, or any comments or questions about corrections, updates, modifications or amendments to this Policy should be directed to IDscript, as provided in Section 1.5 of this Policy.

8.2 General.

All other policies and procedures concerning maintenance and changes to this Policy are under the direction and control of IDscript and DST as determined by agreement between IDscript and DST.