MCDR RELYING PARTY AGREEMENT

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALIDATING MCDR DIGITAL CERTIFICATES, USING MCDR'S ONLINE CERTIFICATE STATUS PROTOCOL ("OCSP") SERVICES, ACCESSING OR USING MCDR DATABASE OF CERTIFICATE REVOCATIONS OR RELYING ON ANY MCDR CERTIFICATE-RELATED INFORMATION. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR RELY ON ANY MCDR INFORMATION. IN CONSIDERATION OF YOUR AGREEMENT TO THESE TERMS, YOU ARE ENTITLED TO USE THE MCDR INFORMATION AS SET FORTH HEREIN.

IN THIS AGREEMENT ALL REFERENCES TO

(a) "MCDR" SHALL MEAN MCDR, INC. (MISR FOR CENTRAL CLEARING, DEPOSITORY AND REGISTRY)

(b) "ITIDA" SHALL MEAN INFORMATION TECHNOLOGY INDUSTRY DEVELOPMENT AGENCY

(c) "CMA" SHALL MEAN CAPITAL MARKET AUTHORITY

(d) "CASE" SHALL MEAN CAIRO & ALEXANDRIA STOCK EXCHANGE

1. Term of Agreement. This Agreement becomes effective when you submit a query to search for MCDR Digital Certificate, or rely on any MCDR Information in the manner set forth in the preamble above. This Agreement shall be applicable for as long as you use MCDR Digital Certificate or rely on any MCDR Information.

2. Definitions.

"Certificate" or “Digital Certificate” means a digital representation of information which at list identifies the certification authority issuing it, names or identifies public key, identifies its operational period, contains a certificate serial number, and is digitally signed by the certification authority issuing it (MCDR).

"Certification Authority" or "CA" means an entity authorized to issue, suspend, or revoke Certificates. For purposes of this Agreement, CA shall mean MCDR.

"Root Certificate Authority" or "Root CA" in a hierarchical PKI, the CA whose public key serves as the most trusted datum for a security domain. For purposes of this agreement, Root CA shall mean ITIDA (Information Technology Industry Development Agency)

"Private Key" the signing key pair used to create a digital signature or the key of any encryption key pair that is used to decrypt confidential information.

"Public Key" the signing key pair used to validate a digital signature or the key of an encryption key pair that is used to encrypt confidential information.

"Subscriber" a subscriber is an entity contracting with MCDR CA for certificate issuance on behalf of one or more subjects.

"Subject" a subject is an entity that is the subject named or identified in a certificate issued to that entity, holds a private key that corresponds to the public key listed in the certificate, and does not itself issue certificates to another party.
A subject may be a Subscriber acting on its own behalf.

“Certification Practice Statement” or “CPS” means a document, as revised from time to time, representing a statement of practices a CA employs in issuing, suspending, revoking and renewing Certificates. MCDR’s CPS is published at www.MCDR.com/repository/cps.

"Certificate Revocation List "or "CRL" a list maintained by a CA of the certificates which it has issued that were revoked prior to their stated expiration date.

"Repository" A trustworthy system for storing and retrieving certificates or other information relevant to certificates. It may also be referred to as a directory.

"MCDR PKI" means the Certificate-based public key infrastructure governed by the MCDR certificate policies, which enables the deployment and use of Certificates by MCDR, its affiliates, their respective customers, Subscribers and Relying Parties.

"Relying Party" means an individual or organization that acts in reliance on a certificate or digital signature.

3. Informed Decision. You acknowledge and agree that: (i) you have sufficient information to make an informed decision as to the extent to which you choose to rely on the information in a Certificate; (ii) your use of or reliance on any MCDR Information is governed by this Agreement and you shall bear the legal consequences of your failure to comply with the obligations contained herein. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A CERTIFICATE.

4. Certificates. MCDR offers two distinct types of certificate services, with each type providing specific functionality within the MCDR PKI:

(a) **MCDR General Certificates** are issued to subscribers to provide digital signature of documents or data in accordance with the Egyptian law no 15 of 2004 and Ministry of Communications and information Technology Decree no 109 of 2005.

(b) **MCDR restricted certificates** are issued to subscribers in particular to digitally sign transactions to be processed through the systems of MCDR, CASE, CMA and other participants in the Egyptian capital markets.

These Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has requested the Certificate Application, and that the subject submitting the Certificate Application on behalf of the Subscriber was authorized to do so.

These Certificates can either be **value limited** or **unlimited**.

5. Your Obligations. As a Relying Party, you are obligated to ensure the reasonableness of your reliance on any MCDR Information by:
(a) Determining that the certificate will be used for an appropriate purpose.
(b) Utilizing the appropriate software and/or hardware to perform digital signature verification.
(c) Identifying a certificate chain and verifying the digital signatures on all certificates in the certificate chain (verifying MCDR certificate signature as CA- verifying ITIDA certificate signature as Root CA)

(d) Checking the status of a certificate in which you want to rely by downloading the last version of the CRL to verify the certificate has not been revoked or suspended.
(e) Verifying the certificate validity period.
(f) Verifying the type of the certificate (General or Restricted)
(g) Verifying the value limit of the certificate.
(f) Rely on the certificate, if all of the checks described in the previous paragraphs are successful, provided that reliance upon the certificate is reasonable under the circumstances and in light of section 3 of this agreement. It is your responsibility if you need to obtain additional assurances for such reliance.

6. Limitations on Use. 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 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.

7. MCDR Warranties. MCDR warrants to Relying Parties who reasonably rely on a Certificate that (i) all information in the Certificate, except for Non-verified Subscriber Information, is accurate as of the date of Certificate issuance; (ii) Certificates appearing in the Repository have been issued to the individual, organization, or device named in the Certificate as the Subscriber; and (iii) the Certificate was issued in substantial compliance with the **MCDR CPS**.

8. MCDR Responsibility MCDR is not responsible for any loss or damage or harm that may result from misusing the service and is not committed to any compensation.

9. Governing Law. Any disputes related to this Agreement shall be governed in all respects by and construed in accordance with the Egyptian Law no 15 of 2004 and Ministry of Communications and Information Technology Decree no 109 of 2005 and the rules issued by ITIDA.

MCDR has the right to modify the terms and conditions of this agreement.
MCDR Relying Party Agreement Version 1.0