Proof SM

DIGITAL CERTIFICATE SUPPLEMENT

This Digital Certificate Supplement is attached to and incorporated into the Proof General Terms ("**General Terms**"). Capitalized terms not otherwise defined have the meanings given in the General Terms, the Proof Glossary, or the Order Form.

1. Applicability. This Digital Certificate Supplement applies to a User, if Proof provides the User with a Digital Certificate.

2. General. Proof will use commercially reasonable efforts to verify the information provided by User when requesting a Digital Certificate (an "**Application**"). If Proof accepts User's Application, Proof will provide the Digital Certificate to User subject to the terms, conditions, and restrictions stated in the Agreement. Proof has no obligation to provide the Digital Certificate to User. Proof will tell User the length of time that the Digital Certificate is valid. At the end of that validity period, User must submit a new Application for a Digital Certificate.

3. Obligations and Restrictions on Use.

3.1 Protection of Private Key. User must protect the Private Key included in a Digital Certificate. A "**Private Key**" means part of a key pair, along with the corresponding public key, that is kept secret. User must take all reasonable measures to protect User's account, Private Key, and any associated activation data or device (such as a password, pass phrase, or token) from unauthorized use and disclosure.

3.2 User's Obligations. As a condition of issuance and use of a Digital Certificate, User acknowledges and agrees that User must:

(a) provide accurate and complete information as part of the Application;

(b) request revocation of the Digital Certificate, if information, to include name and email address, provided by User changes or if User discovers or suspects that User's Private Key was misused or compromised;

(c) notify Proof if User discovers or suspects that User's Proof account has been compromised;

(d) fully cooperate with Proof by providing information, assistance, and cooperation as a result of any compromise of the Digital Certificate or the Private Key;

(e) not use the Digital Certificate for any purpose other than the purpose(s) designated by Proof; and

(f) use the Digital Certificate in accordance with all applicable laws and regulations.

4. Representations and Warranties. User represents and warrants that User: (a) provided true and correct information in the Application and there is no additional information necessary to make the information submitted materially accurate and complete; (b) has the full legal right and authority to obtain a Digital Certificate; (c) has protected and secured the Private Key; and (d) has full legal rights to use the Digital Certificate as part of the Proof Services.

5. Revocation.

5.1 Revocation. Proof, in its sole discretion, may revoke a Digital Certificate if Proof discovers or reasonably suspects that the Digital Certificate or any element of the Digital Certificate: (a) has been compromised; (b) is being used in connection with any illegal activities, such as phishing attacks or fraud; (c) is being used in connection with activities that violate industry norms for acceptable network use, such as hate speech, defamation, intellectual property infringement, non-consensual sex acts or child pornography, network abuse, bulk correspondence (spam), etc.; (d) the continued use of the Digital Certificate presents a risk to the security or integrity of the public key infrastructure ("**PKI**") or presents any other risk to its business, its reputation, Relying Parties, or other users; (e) User is engaged in conduct that is illegal or would be grounds for revocation of the Digital Certificate under this Digital Certificate Supplement; or (f) other grounds stated in documents maintained by Relying Parties. Revocation of the Digital Certificate may also be backdated to protect Internet users and the PKI. "**Relying Parties**" include any and all entities that rely upon the information contained within the Digital Certificate.

5.2 Other. In addition, a Digital Certificate may be revoked, if Proof ceases doing business or is no longer allowed to issue Digital Certificates and no other certificate provider is willing to provide revocation support.

5.3 Expired and Revoked Certificates. User may not use any revoked or expired Digital Certificate. User may not use any Private Key associated with User's revoked or expired Digital Certificate(s) except to decrypt previously encrypted data associated with User's Private Key.

6. Indemnification. User will indemnify, defend, and hold Proof, its affiliates and their officers, directors, employees, agents and representatives harmless from and against any and all costs, damages, liabilities or expenses (including reasonable attorneys' fees) arising from any third-party claims resulting from (a) User's misrepresentation of, or omission, of any material fact in the Application or otherwise submitted to Proof for purposes of the Digital Certificate, regardless of whether such misrepresentation or omission was intentional or unintentional; (b) the compromise or unauthorized use or disclosure of a Digital Certificate or a Private Key; and (c) User's misuse of a Digital Certificate or Private Key. User's obligations under this Section 6 are conditioned on Proof: (x) giving prompt notice of the claim to User, (y) granting sole control of the defense or settlement of the claim to User, and (z) providing reasonable cooperation to User at User's request and expense. Proof may participate in the claim's defense at its sole cost and expense. User will not enter into any settlement that adversely affects Proof's interests without prior written approval, not to be unreasonably withheld. User is not responsible for any settlement it does not approve in writing.

* * * *