Digital Card Solution Schedule

The Agreement for Entrust's Digital Card Solution is made up of these terms (Digital Card Solution Schedule), the General Terms available at https://www.entrust.com/general-terms.pdf, and an Order for such Services. Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. Overview.

1.1 Entrust develops white-label digital banking capabilities addressed to financial institutions issuing payment cards or retailers. These digital banking capabilities allow the digitization of payment cards. End users can be provided with mobile applications, allowing them to make face to face contactless payment or secure e-commerce transactions;

1.2 Customer wishes to offer its customers a digital wallet allowing them to pay with Scheme cards under dematerialized form, using their existing wallet application;

2 Definitions.

2.1 **Authorized Users:** means the individuals entitled by Customer to use the Hosted Service for administering and developing purposes on Customer's behalf pursuant to the terms and conditions of the Agreement.

2.2 **Applicable Law:** means (i) any and all laws, statutes, orders, rules, regulations, directives and codes of conduct and mandatory guidelines in each case which have legal effect, whether local, national, international or otherwise existing from time to time; and (ii) any other similar instrument which is legally binding; applicable to the supply and receipt of the Hosted Service from time to time (including those coming into effect after the Effective Date and in each case as repealed, amended or varied from time to time), but excluding the Scheme Rules.

2.3 **Back-Office:** means the managing and monitoring features available to administer the Hosted Service and manage the life cycle of the End-Users application.

2.4 **End User:** means an individual who is entitled to use Customer's Wallet application which integrates the Hosted Service.

2.5 **Hosted Service:** has the meaning set forth in the General Terms and for the purpose of this Schedule includes the mobile payment SaaS services provided by Entrust as further described in the Order.

2.6 **PCI-DSS:** means the Payment Card Industry Data Security Standard, defined by the Payment Card Industry Security Standards Council, being a common set of internationally applicable requirements specifically designed to provide protection of cardholder data and to ensure that companies that process, store, or transmit cardholder data maintain a secure environment.

2.7 **Renewal Period:** means subsequent subscription periods after the initial Offering Term period of the Offering Term, as set forth in the Order.

2.8 **Scheme Rules:** means the by-laws, rules, operating regulations, certifications, and other instructions issued by the Scheme as may be amended or varied from time to time.

2.9 **Scheme(s):** means the payment schemes operated by Visa, MasterCard or by any other company as agreed between the parties during the Offering Term.

2.10 **Service:** means collectively the Hosted Service, Technical Resources, and Back-Office tools provided by Entrust pursuant to the Order.

2.11 **Service Levels:** means the commitments of Entrust in terms of availability, maintenance, and support of the Service as set forth in the DCS Service Level Agreement and Support Terms available on Entrust's website at https://www.entrust.com/legal-compliance/terms-conditions/digital-card-solution.

2.12 **Technical Resources:** means collectively the API to connect the Customer's system to Entrust's Hosted Services, the back-office website allowing Customer and Authorized Users to operate the Hosted Service, online documentation for the Hosted Service and the SDK, as further detailed in the Order.

2.13 **Token Service providers (or "TSP"):** Token Service Providers are services managed by a third-party. They allow card issuers and merchants to turn regular card numbers into digital tokens. These tokens increase security for both cardholders and merchants. By enabling the digitalization of cards, they bring a key feature, necessary for the proper functioning of the Service.

2.14 **Wallet(s):** means the mobile application developed by the Customer or the Wallet Owner which embedded the Service.

2.15 **Wallet Owner:** means the editor of the application installed on the End User mobile devices for the operation of the digitalized cards.

3 Right to Use, Setup and Implementation.

3.1 Entrust grants to Customer a non-exclusive, non-transferrable right to access and use the Service, including the related documentation for Customer and Authorized Users solely within the frame of Customer's Wallet and for the exclusive benefit of Customer's End Users. This right to use shall only be valid for the duration of the Offering Term.

3.2 Customer shall not use, or permit any person to use, the Service in any way not expressly permitted by the Agreement. Without limiting the generality of the foregoing, Customer shall not:

3.2.1 allow any third party to use the Service (including through outsourcing);

3.2.2 use the Service on behalf of, or for the benefit of, another person except for the benefit of the End Users (including not using the Hosted Service to provide any form of outsourcing, application service provider service, bureau-type service or an equivalent service);

3.2.3 use, integrate or combine the Service with other services or software not installed, provided, or approved by Entrust for purposes other than those contemplated herein; or

3.2.4 copy, reproduce, or transmit to the public any of Entrust Software except for the purposes contemplated herein;

3.3 Customer shall:

3.3.1 ensure that all measures as Entrust may prescribe from time to time for the protection of the Hosted Service from unauthorized use are adhered to by the Customer, the Authorized Users, and End Users; and

3.3.2 notify Entrust immediately of any confirmed or suspected unauthorized access to the Hosted Service.

3.4 Customer acknowledges and agrees that Entrust is entitled to monitor the use and performance of the Hosted Service to ensure compliance with the Service Levels and with all security requirements deriving from Applicable Laws and the Scheme Rules to the extent applicable to the Hosted Service. In this respect, Entrust reserves the right to access and manage Customer data to the extent exclusively necessary.

3.5 For each Order that requires setup and implementation services to be provided by Entrust, Customer and Entrust shall enter into a statement of work, that covers topics including but not limited to: (i) scope, (ii) project schedules, (iii) dependencies and assumptions, (iv) roles and responsibilities, (v) acceptance procedures, (vi) and change management.

4 Data Security.

4.1 The parties acknowledge that in Entrust providing the Service it may collect and process cardholder data. If and to the extent required under PCI-DSS, Entrust shall:

4.1.1 take appropriate technical and organizational measures to protect all data handled by it as a consequence of the Hosted Service against accidental or unlawful destruction or accidental loss, alterations, and unauthorized disclosure or access in accordance with the PCI-DSS certification requirements; and

4.1.2 use reasonable commercial endeavors to protect data from virus infection or third-party intervention.

4.2 Customer acknowledges that Entrust may have access to the Back-Office when it has reason to believe that an event of any sort whatsoever threatens or is likely to threaten the stability of the Hosted Service.

4.3 In the case of a suspected or actual security incident, Customer acknowledges that Entrust may restrict, limit, or suspend the Hosted Service to the extent necessary to address the security incident, without prior notice or indemnity to Customer, and without the Customer being entitled to any damages. Entrust shall keep Customer informed of the extent of the restriction, limitation, or suspension of the Hosted Service.

5 Pricing Changes. Customer acknowledges that Entrust reserves the right to modify the fees for the Service subject to ninety (90) days' notice prior to the end of the initial Offering Term or Renewal Period. Within the initial Offering Term but no more than annually, upon ninety (90) days' notice Entrust may adjust the fees by a percentage equal to the average increase in the Consumer Price Index All Urban Consumers (CPI-U), as calculated by the U.S. Bureau of Labor Statistics, over the prior twelve (12) months.

6 Entrust Obligations.

6.1 Entrust shall at all times throughout the Offering Term:

6.1.1 use commercially reasonable efforts to maintain for a minimum of two (2) years the backward compatibility of Technical Resources subject to the occurrence of any security constraint, Schemes or regulation imposed on Entrust to modify the Hosted Service within shorter period of time;

6.1.2 provide technical maintenance and support services in accordance with Service Levels;

6.1.3 use commercially reasonable efforts to perform its obligations under the Agreement with all due care, skill and diligence and in accordance with the Service Levels and the other terms of the

Agreement; by using at all times appropriately experienced, knowledgeable, qualified and trained staff;

6.1.4 comply with its obligations hereunder, taking into account any demonstrable dependencies on Customer's performance of its obligations under the Agreement; and

6.1.5 use commercially reasonable efforts to maintain its PCI-DSS and Schemes certifications.

7 Customer Obligations.

7.1 Customer shall at all times throughout the Offering Term:

7.1.1 perform Customer obligations described in the Agreement, including this Schedule and the Appendices, and other such obligations reasonably requested by Entrust in order for Customer to receive the Service;

7.1.2 provide reasonable assistance to Entrust in order to enable Entrust to perform its obligations under the Agreement, and ensure that Customer systems are compatible with the Hosted Service;

7.1.3 ensure that the terms and conditions of the Wallet do not exceed the commitments undertaken by Entrust under the Agreement;

7.1.4 comply, and procure its Authorized Users and End Users compliance, at all times with the technical and security requirements and the terms of use provided by Entrust from time to time, including but not limited to: (i) assign each Authorized User a unique and personal ID and ensure that each person who can access the Back Office has and uses the ID which has been assigned to them; (ii) monitor carefully any action affecting Authorized User's IDs, including any addition, deletion, or modification credentials, and other items used as identifier and immediately revoke access for any Authorized User ID attributed to a user which is no longer authorized to access the Back Office for any reason whatsoever; (iii) use best efforts and take reasonable measures necessary to maintain a reasonable level of requests or connections to Entrust Back-Office; and (iv) not perform any penetration tests or load tests of the Hosted Service without the prior written consent of Entrust.

7.1.5 to use a maintained version of the Technical Resources. If Customer fails to do so, Entrust shall not be liable to Customer for any malfunctions, security breaches, or application certification issues.

7.2 Customer acknowledges that any delay or failure to perform its obligations under the Agreement may affect or delay Entrust's performance and ability to deliver the Service and Entrust shall have no liability to Customer for such result.

7.3 Customer acknowledges that it is responsible for its Authorized Users and End Users use of the Service and failure to comply with the terms of use of this Agreement or otherwise provided by Entrust.

8 Disclaimer of Warranties.

8.1 Entrust shall not be held liable for causes which are beyond its control, including but not limited to:

8.1.1 in case of default or failure of any third parties acting on behalf of Customer, or in case of misuse of the Service by a third party including but not limited to the internet operator, the software developer of Customer or the TSP;

8.1.2 in case of dysfunction of the equipment of Customer, the TSP, the Wallet Owner or any service providers acting on behalf of Customer;

8.1.3 unauthorized use of the Hosted Service, unauthorized disclosure, loss or theft of the access code(s) to the Back Office, and, use of the Hosted Service by an unauthorized person;

8.1.4 loss of Customer data or any other damage due to an event that is not attributable to Entrust, including but not limited to theft, destruction, fire, vandalism, hacking, and computer fraud; and

8.1.5 Customer's non-compliance with Entrust's direction of use of the Service.

8.2 Customer acknowledges that the software and Hosted Service is not error or defect free and agrees that the existence of errors and defects in the Hosted Service shall not constitute breach of the Agreement.

9 Intellectual Property.

9.1 Entrust does not assign any intellectual property rights (e.g. patents, copyrights, trademarks, inventions, formulae, trade secrets, etc.). Neither party may assert ownership over the other party's intellectual property rights.

9.2 Customer shall grant to Entrust and its subcontractors all necessary licenses during the Offering Term to the extent necessary for Entrust to perform its obligations under the Agreement and to provide the Service.

10 Compliance with Laws and Scheme Rules.

10.1 Entrust shall:

10.1.1 comply with Applicable Laws and Scheme Rules to the extent to which the Applicable Laws or Scheme Rules apply to Entrust as a provider of the Service under the Agreement;

10.1.2 obtain and comply with any regulatory consent, approvals, licenses, permissions, permits, and authorizations reasonably necessary for Entrust to provide the Service in accordance with the terms of the Agreement; and

10.1.3 be liable for the costs of any change made to the Service as a result of a change to or requirement of Applicable Laws and/or Scheme Rules after the Effective Date but only to the extent they regulate Entrust directly as provider of the Service or operation of its business.

10.2 Customer shall:

10.2.1 comply with Applicable Laws and the Scheme Rules to the extent to which the Applicable Laws or Scheme Rules apply to Customer as recipient of the Service under the Agreement;

10.2.2 obtain and comply with any regulatory consents, approvals, licenses, permissions, permits, and authorizations reasonably necessary for Customer to receive the Service in accordance with the terms of the Agreement;

10.2.3 ensure that the Wallets comply with all applicable Scheme Rules;

10.2.4 advise Entrust on any specific request or directive made to it by an relevant Scheme or any regulator concerning the Service, or of any changes or proposed changes in the Scheme Rules and Applicable Laws of which they become aware of and may affect the Service.

10.2.5 be liable for the costs of any changes made to the Service as a result of a change to or requirement of Applicable Laws and/or Scheme Rules after the Effective Date to the extent they regulate Customer directly in its capacity as recipient of the Service or Customer's operation of its business.

10.3 The parties agree to provide reasonable co-operation and assistance to each other to resolve issues relating to compliance with Applicable Laws and Scheme Rules, including providing such information as may be reasonably required in connection with the requests from regulators.

11 Feature Specific Terms

11.1 Decision Recommendation Feature:

11.1.1 Description. Entrust may make available, as part of the Service, an optional decision recommendation feature (the "Decision Engine") that generates authorization outcome recommendations (e.g., approve, challenge/authenticate, or decline) based solely on data received from the TSP. The Decision Engine does not independently collect, verify, or supplement the data provided by the TSP.

11.1.2 Advisory Nature; No Transfer of Responsibility. All recommendations generated by the Decision Engine are advisory only and are intended solely to assist Customer in exercising its own independent judgment. All final decision-making authority and responsibility with respect to authorization outcomes remain exclusively with Customer as the issuing bank or its designee. No recommendation generated by the Decision Engine shall be construed as: (a) a binding instruction or directive to Customer; (b) a guarantee of any particular outcome; or (c) an assumption by Entrust of responsibility for Customer's authorization decisions or a transfer of decision-making authority from Customer to Entrust.

11.1.3 Customer Acknowledgement. By activating or using the Decision Engine, Customer acknowledges and agrees that: (i) it has independently evaluated the suitability of the Decision Engine for its operations; (ii) Customer is solely responsible for all authorization decisions, including those made with reference to a recommendation generated by the Decision Engine; (iii) Customer shall not implement automated authorization processes that rely exclusively on Decision Engine recommendations without maintaining independent human oversight in compliance with Applicable Laws, Scheme Rules, and applicable regulatory requirements; and (iv) the disclaimers, limitations of liability, and indemnification provisions set forth in the General Terms and this Schedule apply in full to the Decision Engine and all recommendations generated thereby, including without limitation, Entrust's disclaimer of warranties with respect to third-party data sources such as the TSP.