



Tel: (240) 535-2095 ◆ <http://mobile.setecs.com> ◆ E-mail: sead.muftic@setecs.com

SETECS® SAFE™ System

COOPERATION AGREEMENT for the SAFE™ System in [Country]

This COOPERATION AGREEMENT is established by and between **SETECS® Mobile Technologies**, fully owned subsidiary of **SETECS®, Inc.**, US Corporation (DUNS Number: 147865781, EID/TIN Number: 20-091-5348), with offices located at 5801 Nicholson Lane, Suite #1233, North Bethesda, MD 20852, USA (herein further referred to as "**SETECS® Mobile**") and **[System Operator], [Country]** company, located at _____ (herein further referred to as "**Partner**"). SETECS® Mobile and **[Partner]** are collectively in this document referred to as "**Partners**".

WHEREAS, SETECS® Mobile

- has developed, licenses and deploys components, technologies and products, collectively known as "**SAFE™ system**", for secure mobile transactions and applications,
- provides expertise, software products, and software, security and operational services for installation, activation, customization, and deployment of the SAFE™ system,
- wants to establish and operate secure mobile transactions system in **[Country]** and to offer services to the customers in **[Country]**.

WHEREAS, **[Partner]**

- currently offers **only standard banking and other financial services in [Country]**,
- wants to use SAFE™ system in order to provide to its current and future customers secure mobile financial services based on use of the SAFE™ system.

THEREFORE, based on all of the above, SETECS® Mobile and **[Partner]** have agreed as follows:

1. The Principles of the Cooperation Arrangements

1.1 SETECS® Mobile and **[Partner]** will establish close cooperation and partnership in order to provide various secure mobile financial services in **[Country]** based on use of the SAFE™ system. This Cooperation Agreement establishes technical, business, organizational, legal and financial framework for joint activities of the Partners related to the planning, installation, customization, activation, promotion, marketing, demonstration, operation, and provision of all other supporting services of the secure mobile financial transactions system in **[Country]**.

1.2 The main principle of the partnership is close cooperation beyond standard client-vendor commercial relationships model. This means that Partners will jointly plan, install, promote, operate and perform jointly all other activities of the system, in accordance to their roles. For their joint activities, when appropriate, Partners may establish joint working teams, planning groups, and other ad-hoc joint cooperation forms.

1.3 Partners will jointly create, consider, adopt and follow all financial arrangements related to the SAFE™ system in **[Country]**, such as, but not limited to, setup costs, operational costs, pricing, revenue distribution, investments in expansion and other aspects relevant for operations of the system.

For **SETECS® Mobile**:

For **[Partner]**:

1.4 In case of interest for external funding – equity and/or any other type of investment or in case of opportunities to receive grants, Partners may consider establishing joint venture, shared ownership, mutual investments or any other form of closer cooperation for the future expansions of the system.

1.5 In case of market demands and market opportunities and if [Partner] has products and/or technologies that are either identical or complementary to SETECS® Mobile products, the Partners will jointly consider and decide:

- in case of complementary products or technologies, how to integrate them into the global SAFE™ system;
- In case of overlapping products or technologies, which product to include in the instance of the SAFE™ system to be delivered to the particular customer.

In this process the Partners will discuss and jointly decide on all technical, organizational, and financial aspects of this integration. In case of joint development of new secure mobile products, the Partners will discuss and jointly decide the terms of joint ownership of the intellectual property rights of such products.

1.6 In case of existence or joint pursuit of certain certification and compliance standards, market demands for such certification, or mutual business interest of the Partners, the Partners will cooperate closely in the process of such certification. In this process the Partners will discuss and jointly decide on all technical, organizational, and financial aspects of this certification.

2. Objectives and Scope of the Cooperation

2.1 The objective of this Agreement and the goals of cooperation between Partners are to provide products and services for secure mobile financial, banking, commerce, air-time, ticketing, and other mobile transactions to customers and clients in [Country] – companies and individuals. Potential *customers* are the entire population in the [Country]. Potential *clients* are banks, mobile network operators, telecommunication services providers, Web merchants and other individuals and business entities interested to use mobile services provided by the SAFE™ system.

2.2 In this document and in the concept of the SAFE™ system, the term “*customers*” means *individuals* registered in the SAFE™ system. Merchants and small shop owners are also treated as customers. Customers always use the instance of the SAFE™ system operated by [Partner] as the system operator or jointly by Partners.

2.3 In this document and in the concept of the SAFE™ system, the term “*clients*” means *business entities* that use SAFE™ system to provide access to their services using mobile services of the SAFE™ system. Clients may use an instance of the SAFE™ system operated by Partners (so called *managed services* version) or operated by themselves (so called *deployed* version).

2.4 Within the framework of this Agreement, the scope of services and activities of Partners includes, but it is not limited to, the following:

- *Promotion* – distribution of information about the SAFE™ system in [Country] and internationally, at public events, through public media, conferences, exhibitions, and similar events;
- *Marketing* – direct dissemination of information about mobile services, financial and business benefits, technical features, deployment steps, and operational usage of the SAFE™ system to potential *customers* and *clients* of the system;
- *Demonstration* – installing and running demo version of the SAFE™ system in premises of the [Partner] or at locations of potential clients;
- *Deployment* – running an instance of the SAFE™ system in [Country] for customers – individuals and for clients – companies that select outsourcing of their mobile services to the Partners – *managed services* version of the SAFE™ system;
- *Installation* – assisting clients that want to install and operate their own instance of the SAFE™ system with installation and configuration of the system components and their

- eventual customization to the local environments – *deployed* version;
- *Launching* – assisting clients with initial setup and activation of the SAFE™ system components and first transactions for the deployed versions;
- *Supporting Services* – providing infrastructure components and services for identification, authentication, certification, authorization and federation services;
- *Operation* – providing mobile services to customers and those clients that select managed services option;
- *Software Services* – maintenance and upgrades of the SAFE™ system software modules for customers using deployed version.

2.5 Besides operational objectives of this Agreement, stated in section 2.1, strategic objective of this Agreement is to establish close cooperation and partnership between the Partners, which will be reflected through joint planning, promoting, deployment, and operations of the SAFE™ system in [Country].

3. The Roles of Partners, Contributions and Relationships

3.1 The role of SETECS[®] Mobile in this cooperation is to provide technical expertise, software products, software services, and back-end operational services: security and servers support. Five groups of secure mobile services available at the time of signing this Agreement are specified in Appendix A. Products that SETECS[®] Mobile will provide are specified in Appendix B, section B.1.1. Services that SETECS[®] Mobile will provide are specified in Appendix B, section B.1.2.

3.2 The role of [Partner] is to provide software and hardware prerequisites and promotion, marketing, and front-end operational services, as specified in the Appendix B, section B.2.

3.3 As its contributions to this initiative, SETECS[®] Mobile will provide to [Partner] in the setup phase the right to use (license, free of charge) all of its SAFE™ system software components and products needed to establish an instance of the Basic Version of the SAFE™ system for [Country]. Basic Version supports only transactions based on mobile accounts (SAFE™ accounts) and uses only SMS messages. SETECS[®] Mobile will also provide in the setup phase all software development, upgrades, extensions, customizations, installation, configuration, activation and improvement activities, as needed for the successful launch of the SAFE™ system in [Country]. If [Partner] does not have capabilities to customize SAFE™ Web Server GUI, SETECS[®] Mobile will perform that task, charging real costs to [Partner]. In the deployment phase SETECS[®] Mobile will charge for licensing of its products and for its services, as specified in section 6 of this Agreement.

3.4 As its contributions to this initiative, [Partner] will provide in the setup phase all necessary hardware and software prerequisites and all labor activities for the successful launch of the SAFE™ system in [Country], as needed. [Partner] will also pay initial operational costs for:

- customization of the SAFE™ Web Server GUI for [Partner], if [Partner] does not have persons and capabilities to modify SAFE™ Web Server GUI by itself; and
- the first bulk of SMS messages.

In the deployment phase [Partner] will provide coordination activities with system agents and all its current contacts, activities and customers interested to use mobile services of the SAFE™ system. In the deployment phase [Partner] will charge for its services, as specified in section 6 of this Agreement.

3.5 Initial version of this Agreement, relationships of the Partners and all cooperation activities are **not exclusive**. For SETECS[®] Mobile, this means that it may license its products and may provide its mobile services to other partners, customers and clients in [Country], except to customers and clients of [Partner]. For [Partner], this means that it may use other software vendors for some of its mobile services, except for software products and services provided by SETECS[®] Mobile under this Agreement. [Partner] will not develop its own software for mobile services, and it will direct all its customers, interested in secure mobile services to SETECS[®] Mobile. This principle means that [Partner] will be a provider of secure mobile services and also reseller for deployed versions of the SAFE™ system in [Country].

3.6 This Agreement will be automatically converted to an exclusive Agreement for [Country] for the period of one year, when [Partner] signs Deployment Agreement/Contract with one telecom operator and one bank, if by that time SETECS® Mobile has not signed equivalent Cooperation Agreement with some other partner. One year after conversion to exclusive Agreement, exclusivity will be automatically extended for the next year, if the revenue in the second six months of the previous year exceeds revenue in the first six months of the previous year.

4. System Operations

4.1 After signing this Agreement, the Partners will immediately establish an operational version of the SAFE™ system in [Country]. Servers will be hosted by [Partner] in its premises in [Country] or wherever decided by [Partner]. SAFE™ Administrative Stations will be located both in [Country], operated by [Partner] and SETECS® Mobile team in [Country] and in the USA, operated by SETECS® Mobile team in the USA for its software and security services. If SAFE™ smart cards are introduced, SAFE™ CMS Stations and SAFE™ CMS Server will be located in [Country] and operated either by [Partner] or by the SETECS® Mobile team in [Country].

4.2 Initially, the system will provide five groups of secure financial services, as specified in Appendix A and in the “SAFE™ System Description” document. Later, the system may be extended with new mobile services, such as mobile microfinance, mobile ticketing, mobile parking, mobile Government services, m–health, and other mobile services, if there is interest of customers in [Country].

4.3 Initially, until the system starts creating revenue, the Partners will support system operations with their existing team members. Later, when the system starts building revenue or any other financial support for its operations is obtained, the Partners may recruit new members of the Management and Operational Team to support system operations. The number of new members of the team, their roles and functions, compensation and other issues will be jointly decided by the Partners.

4.4 SETECS® Mobile will establish and maintain SAFE™ Web Server for [Country] to promote, access to and use the functions of the SAFE™ system. Since Web pages will also be used for services offered by SETECS® Mobile (software downloads, management of certificates, etc.), SETECS® Mobile will coordinate design, creation, and maintenance of the SAFE™ Web Server for [Country]. [Partner] may provide advice, recommendations and suggestions for layout and functionality of the SAFE™ Web Server in [Country] and may also perform customization of Web pages, if so agreed between SETECS® Mobile and [Partner].

4.5 For marketing and promotion of the SAFE™ system in [Country], the Partners will jointly design various printed materials (leaflets, brochures, posters, etc.). [Partner] will be in charge of printing and distribution of these materials.

5. Governance and Management

5.1 The Partners will jointly manage an instance of the SAFE™ system in [Country].

5.2 Upon deployment and activation of the system, if needed, the Partners will jointly organize creation and adoption of all business documents required by the [Country] laws for legal operations of the system in [Country], specifying compliance to financial regulations, limits for transactions and transfers, provisions against money laundering and other potential illegal transactions, , security of the overall system, privacy of users, protection against identity fraud, and other policy and regulatory documents, as necessary.

5.3 In particular, the Partners will jointly establish Financial Policy of the SAFE™ system, specifying transaction fees, their distribution, the principles of automatic clearance, relationships and cooperation with various financial institutions, and other relevant financial aspects, important for operations of the system. Financial Policy of the system will be based on SETECS® Mobile’s Financial Policy model.

For SETECS® Mobile:

For [Partner]:

5.4 The Partners will establish joint Management Team for the system. The primary role and responsibility of the Management Team is to consider and approve external expenses covered by the 34% of the system revenue.

5.5 Initially, Management Team will have four members: Sead Muftic and Gernot Schmoelzer (as representatives of SETECS® Mobile) and [TBD and TBD] (as representatives of [Partner]). As soon as financial resources are available for compensation, if needed, the Partners will mutually agree and engage one more member of the Management Team who will be full-time, professional Project Manager for the SAFE™ system.

5.6 The Partners will jointly decide and engage external consultants, if needed.

5.7 In order to keep its own financial resources, each Partner will open its own, regular business account in some commercial bank in [Country]. In addition, in order to keep pre-paid amounts (deposits) of customers to their SAFE™ accounts, [Partner] will open and maintain one additional standard business banking account. This account will be used as SAFE™ system escrow account.

5.8 [Partner] will be in charge of the administration of the SAFE™ escrow account. This means that [Partner] will nominate one or more authorized account administrator(s) who will be in charge of and will perform all financial transactions with the SAFE™ system escrow account.

6. Financial Arrangements

6.1. Setup Phase – SETECS® Mobile: For the setup phase SETECS® Mobile will provide all the necessary software components needed for installation, customization, initial testing, and activation of the system. Additionally, SETECS® Mobile will also provide technical services during the setup phase to install its SAFE™ system software and to install its IDMS and CA Servers. Software will be licensed free of charge and services will be provided for free, if performed remotely.

6.2. Setup Phase – [Partner]: For the setup phase [Partner] will be responsible for the costs of its team members, for costs of all software and hardware prerequisites and for initial setup costs. These costs include, but are not limited to:

- Costs for hosting hardware components either in the premises of the [Partner], with some hosting provider in [Country] or by some hosting provider in the USA, should [Partner] at its sole discretion, choose to host the hardware components outside of [Country]
- Setup costs for connecting to the SMS Gateway and for obtaining/maintaining system's short code and / or long mobile numbers.
- Operational costs for sending/receiving SMS messages, until those costs are charged to users.
- The costs of customization of the SAFE™ Web Server, if SETECS® Mobile will perform this task.

6.3. Setup Phase – Real Costs: In principle, in the setup phase, if local presence, visits and activities of the members of the SETECS® Mobile team in [Country] are not needed, each Partner will cover its own labor costs. It is expected that [Partner] will cover SETECS® Mobile real costs in the setup phase, if those are incurred. If visits to [Partner] locations of the members of the SETECS® Mobile technical or business team are needed, then [Partner] will cover real costs of those activities – travel, hotel, local transportation, and per-diem reimbursements.

6.4 Deployment Phase: Financing of operations, maintenance and expansions of the fully functional SAFE™ system during its deployment will be based on the following principles:

- (a) Partners will jointly establish the prices and pricing principles for system services, based on SETECS® Mobile's Financial Policy model;
- (b) Partners will jointly decide on the policy for charging transaction fees, including offering various benefits and discounts;

- (c) Partners will jointly decide who will be the payer for each transaction/service and all other arrangements and principles for compensation of system services,
- (d) If sharing of SMS fees is agreed with the aggregator or supporting telecom operators, shared portion of SMS fees will be equally distributed between two Partners;
- (e) Total revenue from all operations and services will be used to cover external costs of system operations and to share the profit between Partners;
- (f) For the first year of operations external costs will be planned at the 34% of the total revenue;
- (g) In the first year of operations the Partners will plan equal sharing of the profit, i.e. at 33% for each Partner. This means that transaction fees will be divided to operational external costs (34%), [Partner]'s portion (33%) and SETECS® Mobile's portion (33%);
- (h) These principles will be evaluated and eventually adjusted at the end of each year of operations.

6.5 External Services and Costs: 34% of total system revenue or the amount agreed by the Management Team will be used to cover external costs of system operations. External costs include four categories:

- Reimbursement to system agents for registration of subscribers, if required, if agreed with agents, and if such reimbursement is planned in the Financial Policy;
- Reimbursement to merchants for accepting SAFE™ payment transactions, if such reimbursement is planned in the Financial Policy;
- Reimbursement to communication aggregator or supporting telecom for outgoing SMS, GPRS or any other type of outgoing messages;
- Reimbursement of SETECS® Mobile's local taxes if SETECS® Mobile portion of transaction fees is less than 33%.

6.6 Revenue from Deployed Versions: If SAFE™ system is used as a deployed version, operated by some client arranged by [Partner], then the company operating the system will be treated as system operator. This means that SETECS® Mobile will establish partnership and cooperation agreement with such client equivalent to relationships with [Partner] regulated by this Agreement. In this case [Partner] will be treated as Country Representative. This means that SETECS® Mobile will pay 10% of the 33% of SETECS® Mobile's revenue to [Partner]. All other relationships (licensing of software, services, etc.) will be arranged directly by SETECS® Mobile and the client operating the system.

6.7 Expenses and Overheads: If the portion of total system revenue that belongs to SETECS® Mobile is less than 33%, then all amounts payable by [Partner] to SETECS® Mobile under this Agreement and the associated Software Licensing Agreement are net payments to SETECS® Mobile, exclusive of any tax, withholding tax, levy, or similar governmental charges that may be assessed by any jurisdiction in or outside [Country]. Such taxes, withholding taxes, levies, and governmental charges (collectively "Taxes") include Taxes based on sales, use, excise, import or export values/fees, value-added, income, revenue, net worth, or may be the result of the delivery, possession, or use of the SAFE™ system components and products, the execution or performance of this Agreement or otherwise. Should any Taxes be legally due by SETECS® Mobile, [Partner] agrees either to increment the amount of payments for the amount of Taxes or to pay such Taxes on behalf of SETECS® Mobile and therefore indemnify SETECS® Mobile for any claim for such Taxes demanded. [Partner] shall make no deduction from the portion of transaction fees specified in sections 6.4 and 6.5 owed to SETECS® Mobile for any Taxes.

6.8 For all taxes paid by [Partner] on behalf of SETECS® Mobile, [Partner] shall provide to SETECS® Mobile within forty-five (45) days after the end of any quarter, a certificate of tax payment documenting the payment and amount of the taxes paid during the preceding quarter.

6.9 Local SETECS® Mobile team: If SETECS® Mobile agrees with [Partner] to deploy locally in [Country] the members of its own team, either employees or consultants, temporarily or permanently, all costs of that local supporting team will be paid by [Partner] from the 34% of systems operational costs.

For SETECS® Mobile:

For [Partner]:

6.10 Software Licensing Agreement: SETECS® Mobile and [Partner] will sign Software Licensing Agreement. If the portion of total system revenue that belongs to SETECS® Mobile is 33% or more, then SETECS® Mobile will provide software maintenance and all upgrades free of charge.

6.11 Arrangements: All financial, organizational and business arrangements will be established by mutual consent of both Partners.

7. Registered Trademarks, Trademarks, Copyright, Intellectual Property Rights

7.1 The Partners acknowledge that SAFE™ system and Secure Mobile Wallet™ are trademarks of SETECS® Mobile. SETECS® is registered trademark in the USA. All technical documentation about SAFE™ components and products, distributed by SETECS® Mobile, are owned by SETECS® Mobile. All source code, design solutions, procedures, protocols, database schemas, and security token profiles are owned by SETECS® Mobile and represent its intellectual property.

7.2 The Partners acknowledge that SAFE™ system is the brand, representing security and mobile technologies, products, infrastructure components, protocols, and secure mobile transactions.

7.3 SETECS® Mobile retains all ownership rights to all applicable copyrights, trade secrets trademarks, service marks, trade names and other intellectual property rights in the SAFE™ system. [Partner] will make all reasonable efforts to prevent its customers (i) to copy, modify or reproduce any SAFE™ component or accompanying documentation in any way without explicit written permission by SETECS® Mobile, (ii) to reverse engineer, disassemble, or decompile SAFE™ component, (iii) to remove, obscure or alter the SETECS® Mobile proprietary notices, any accompanying End–User License Agreement or other documentation for SAFE™ component, (iv) to incorporate any SAFE™ component into any other software or hardware product, or (v) to private label any SAFE™ component or any portion thereof or include any other Partner’s marks or legends on any SAFE™ component or any portion thereof. Any documentation accompanying a software product shall also be deemed part of the SAFE™ system and delivered to each end–user as a complete product.

7.4 SETECS® Mobile grants to [Partner] a non-exclusive, royalty-free license to use SETECS® Mobile trademarks, service marks, and trade names for the purpose of advertising, promoting, merchandising and marketing SAFE™ system. [Partner] agrees that all such material relating to the SAFE™ products shall identify SETECS® Mobile as the source of the products and otherwise comply with the Software Redistribution Guidelines, specified in the Software License Agreement and incorporated in this document by reference. [Partner] will discontinue all use of SETECS® trademarks and names promptly upon the termination or expiration of this Agreement.

7.5 SETECS® Mobile has filed several patent applications, currently treated as provisional applications. Applications are for USA and international patents. SETECS® Mobile will introduce the summaries of those applications to [Partner]. By signing this Agreement, [Partner] guarantees to SETECS® Mobile that it will honor and protect those patents and that it will not file competing patent applications.

8. Branding

8.1 [Partner] will honor, use and enforce the branding of the SAFE™ system and all its components.

8.2 SAFE™ smart cards are branded with SETECS® Mobile logo in the lower right corner on the front side of the card. The remaining area of the front side of the SAFE™ smart card and the back of the card are free format and available for [Partner]’s co-branding, if desired.

8.3 SAFE™ Secure Mobile Wallet™ is branded with SETECS® Mobile logo displayed at the icon to start the Wallet, during the startup of the Wallet, when used as mobile phone application or when used as UICC applet. SAFE™ Secure Mobile Wallet™ may be co-branded by [Partner] or by some of

its clients.

8.4 SAFE™ Web Server is branded with SETECS® Mobile logo displayed in the upper left corner of each Web page. SAFE™ Web Server may be co-branded by [Partner] or by some of its clients.

8.5 Certificates are branded as SETECS® certificates, having “SETECS” as an Issuer’s Distinguished Name in each certificate and compliant to the SETECS® Certification Policy.

8.6 All co-branding arrangements for SAFE™ smart cards, SAFE™ Secure Mobile Wallet™, SAFE™ Web Server and SETECS® certificates will be arranged by a separate agreement.

9. Terms and Termination of the Agreement

9.1 This Agreement shall commence on the later date of the two signatures and shall continue for an initial term of three (3) years. Thereafter, this Agreement shall automatically renew for additional one-year periods, unless Partners provide notice of non-renewal of cooperation and participation in system operations at least 90 (ninety) days prior to the renewal date.

9.2 Partners may terminate immediately this Agreement at any time based on the mutual consent without any prior notification.

9.3 Either Partner may terminate this Agreement for its participation in the operations of the system: (a) upon not less than 90 (ninety) days' prior written notice in the event of a material breach of this Agreement by the other Partner and the failure of such other Partner to cure such breach within an additional 30 (thirty) day period; (b) merger or acquisition of the Partner; (c) a receiver is appointed for the Partner or its property; (d) the Partner makes, or attempts to make, an assignment for the benefit of its creditors; (e) any proceedings are commenced by or for the Partner under any bankruptcy, insolvency, or debtor's relief law; or (f) the Partner liquidates or dissolves or attempts to liquidate or dissolve.

9.4 The expiration or termination of this Agreement, for whatever reason, will not discharge or relieve either Partner from any obligation to the other Partner, accrued prior to such expiration or termination, will not relieve any Partner that has breached this Agreement from liability for damages resulting from such breach, and will not destroy or diminish the binding force and effect of any of the provisions of this Agreement that expressly, or by reasonable implication, come into or continue effect on or after expiration or termination hereof.

10. Post-Termination Actions

10.1 Upon expiration or termination of this Agreement for any reason by one Partner, the other Partner will have the right to continue operating the instance of the SAFE™ system established under this Agreement, based on its own decision.

10.2 The terminating Partner will have no rights to withdraw its assets and contributions to the system established before the termination date.

10.3 Upon expiration or termination of this Agreement for any reason, the Partners shall have the following rights and obligations:

- In case of SETECS® Mobile termination, [Partner] will have the right to select another vendor to provide products and services equivalent to those described in Appendix B.1, as appropriate to [Partner]’s post-termination plans. SETECS® Mobile will have obligation to lease products, provide services and participate in operations of the system at most one year after the date of termination of this Agreement.
- In case of [Partner]’s termination, SETECS® Mobile will have the right to maintain all software, hardware and data resources in [Country] established in this project and to find another system operator that will provide the same services, as specified in Appendix B,

For SETECS® Mobile:

For [Partner]:

section B.2. [Partner] will have the obligation to provide to SETECS® Mobile all its resources and services at most one year after the date of termination of this Agreement.

10.4 The due date of all outstanding invoices, if any, shall automatically accelerate so that they become due and payable on the effective date of termination, even if longer terms had been previously provided.

10.5 [Partner] shall not have the right to use SETECS® brand and trade names, trademarks and service marks following the expiration or termination of this Agreement.

11. General Provisions

11.1 This Agreement supersedes all prior agreements, proposals, representations and communications between the Partners relating to the subject matter herein. In the case of conflict between this Agreement and any other previous arrangements created for deployment of the SAFE™ system in [Country], the terms of this Agreement shall prevail.

11.2 The Partners agree that this Agreement and the SAFE™ system products including all information related to the products that is disclosed to the [Partner] as a result of this Agreement, (i) constitutes the proprietary and confidential information of SETECS® Mobile; (ii) shall be used by [Partner] only as required to exercise the activities specified in this Agreement; and (iii) shall be held in confidence and shall not be made available in any form to any person or entity other than [Partner], without the express written consent of SETECS® Mobile.

11.3 In order to eliminate potential conflicts and to guarantee non-circumvention, [Partner] will register with SETECS® Mobile all its clients (see definition in section 2.3). SETECS® Mobile will accept new registrations if they do not represent conflict with other registrations. SETECS® Mobile agrees not to circumvent the [Partner] by entering into negotiations directly or indirectly with companies or individuals identified by [Partner] or its agents, registered and accepted by SETECS® Mobile.

11.4 In case of conflicts and disputes about the system status and its operations, the first attempt will be to resolve them by negotiations in good faith and business spirit. The next approach would be arbitration. Finally, in case of legal procedures, this Agreement shall be interpreted under the laws of USA, if there are no conflicts of law principles. If the dispute is about performance of SETECS® Mobile software or SETECS® Mobile' IPRs, then the US laws will prevail.

11.5 This Agreement is not assignable to any other party without the written consent of the other party, which consent shall not unreasonably be withheld if the receiving party accepts the terms of this Agreement. Any amendments or waivers of this Agreement must be in writing signed by both Partners.

11.6 Exception to section 11.5 is the case if SETECS® Mobile decides to incorporate local company in [Country] with majority ownership, in which case SETECS® Mobile may transfer its rights under this Agreement and is free to regulate relationships between SETECS® Mobile and the local company without consent of [Partner].

11.7 In any action between the Partners to enforce any term of this Agreement, the prevailing Partner shall be entitled to recover reasonable expenses, including reasonable attorneys' fees.

11.8 Any notice required to be given by either Partner to the other shall be deemed given if in writing and actually delivered to the Partner at the address set forth above (including by facsimile and electronic mail).

11.9 If any term of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then this Agreement, including all of the remaining terms, will remain in full force and effect, as if such invalid or unenforceable term had never been included.

For SETECS® Mobile:

For [Partner]:

11.10 This Agreement terminates and supersedes all prior understandings or agreements on the subject matter hereof. This Agreement may be modified only by a further writing that is duly executed by both Partners.

SETECS® Mobile:

[Partner]:

Name: **Sead Muftic**

Name: -----

Title: Chairman/CEO

Title:

Date: _____, 2010

Date: _____, 2010

For **SETECS® Mobile:**

For **[Partner]:**

APPENDIX A: System Functionality

The functionality of the SAFE™ system in [Country] has been described in the document “SAFE™ System Description”. It is briefly summarized in this Appendix for completeness of this document.

Depending on the needs and requirements of clients and customers in [Sweden] the instance of the SAFE™ system will be based either on a standard or customized version of the SETECS® Mobile products, available at the signing of this Agreement, called *Secure Applications for Financial Environments* (“SAFE™ system”). Depending on mobile services offered, the system will be integrated with the existing telecommunication and banking networks in [Country], as appropriate. The system will comprise five subsystems and it will provide the following services to banked and un-banked customers in real-time, in and out of cell phone range:

- **m–Accounts (pre–paid) Transactions** – Mobile payments, account inquiries, and funds transfers; electronic processing of cash-in/cash-out transactions for SAFE™ account holders, primarily un–banked users, but also for banked customers.
- **m–Banking Transactions** – Mobile payments, account inquiries, and fund transfers for bank account holders ([Partner] customers)
- **m–Commerce Transactions** – Processing of customers’ payment transactions over–the–counter (OTC) by merchants registered in the system
- **m–Business Transactions** – Processing of mobile payments transactions by system clients (businesses entities) registered in the system.
- **m–Remittance Transactions** – financial and information dissemination transactions performing financial transfers between two countries (remittance), when an instance of the SAFE™ system is established and become operational in the receiving country.

The fully integrated SAFE™ system will support secure financial transactions processing in [Country], using a comprehensive set of products, including various servers, POS devices, mobile phones and smart cards, described in Appendix B.1.1. The following groups of functions will be provided:

- (a) *Establishment and management of pre–paid SAFE™ Accounts* for individuals ([Partner] agents and subscribers) and for business entities (service providers and merchants);
- (b) *Issuance and management of SAFE™ smart cards* with biometric features for [Partner] agents, customers, and merchants;
- (c) *Use of the SAFE™ smart cards for authentication and authorization* against SAFE™ accounts and for stored money payments,
- (d) *Use of mobile phones to perform various financial transactions,*
- (e) *Use of SAFE™ accounts for financial transactions* – Point–of–Sale (PoS) payments, cash deposits/withdrawals, and account transfers. PoS payment transactions are purchases of goods and services with merchants using over–the–counter (OTC) or over–the–air (OTA) transactions, and
- (f) *International financial transactions – remittance.*

APPENDIX B: Products and Services

B.1 SETECS® MOBILE TECHNOLOGIES

SETECS® Mobile Technologies will be responsible for all software components and software services and for two groups of operational services: security services and back–end operational services.

B.1.1 SETECS® Mobile SAFE™ Products

SETECS® Mobile Technologies products are described in detail in the Software License Agreement, associated to this Agreement, but they are here reproduced for completeness of this document:

1. **SAFE™ IDMS Server** – The server that performs the following functions:
 - 1.1 Registration of customers
 - 1.2 Registration of other SAFE™ Servers
 - 1.3 Registration of external servers
 - 1.4 Distribution of registration data to other SAFE™ Servers
2. **SAFE™ PKI/CA Servers** – Certificate Authority (CA) servers organized in a Public–Key Infrastructure (PKI) hierarchy that perform the following functions:
 - 2.1 Generation of certificates
 - 2.2 Storage of certificates
 - 2.3 Distribution of certificates
 - 2.4 Verification of certificates
 - 2.5 Generation and distribution of CRLs
3. **SAFE™ Card Management System (CMS) PC Station** – The station that performs the following functions:
 - 3.1 Registration of SAFE™ customers for issuance of smart cards
 - 3.2 Enrollment of SAFE™ customers
 - 3.3 Submission of card issuing requests
 - 3.4 Activation of SAFE™ smart cards
 - 3.5 Management and re-issuance of SAFE™ smart cards
4. **SAFE™ Card Management System (CMS) PoS Station** – The station that performs the following functions:
 - 4.1 Issuing of SAFE™ smart cards
 - 4.2 Management and re-issuance of SAFE™ smart cards
5. **SAFE™ Card Management System (CMS) Server** – The server that performs the following functions:
 - 5.1 Storage of card requests and data about issued SAFE™ cards
 - 5.2 Issuance of SAFE™ smart cards (loading of SAFE™ Wallet and other applets, personalization of SAFE™ smart cards, printing of cards, re-issuance of cards)
 - 5.3 Over–the–Air (OTA) provisioning of SAFE™ Wallet and other applets
6. **SAFE™ Production Web Server** – Web server that performs the following functions:
 - 6.1 Registration of SAFE™ customers using Web forms
 - 6.2 Management of SAFE™ security parameters
 - 6.3 Management of SAFE™ user profiles
 - 6.4 Management of SAFE™ mobile accounts
 - 6.5 Management of SAFE™ transactions
7. **SAFE™ Communication Server** – The server that performs the following functions:
 - 7.1 Communication with SMS and / or GPRS Gateways of aggregators and/or telecom providers

- 7.2 Communication with SAFE™ Payment Server
- 7.3 Communication with other SAFE™ Mobile Application Servers (Mobile Ticketing Server, Mobile Bills Server, Mobile Parking Server, Mobile Promotions Server, Mobile Coupons Server, etc.)
- 7.4 Communication with other SAFE™ Communication Servers in other domains (system-to-system communications)
- 8. **SAFE™ Payments Server** – The server that performs the following functions:
 - 8.1 Communication with SAFE™ Communication Server
 - 8.2 Communication with EMV Payment Gateway Server
 - 8.3 Communication with IT processing systems in participating banks and other financial Institutions and financial services providers (remittance, micro-finance, bill payments, etc.)
 - 8.4 Communication with SAFE™ Production Web Server
 - 8.5 Communication with other SAFE™ Mobile Application Servers
- 9. **SAFE™ Administrative Station** – The station that performs the following functions:
 - 9.1 Administration of the SAFE™ IDMS Server – registration and customization
 - 9.2 Administration of the SAFE™ Communication Server – communication channels and configuration parameters
 - 9.3 Administration of SAFE™ Financial Server – registration of banks, accounts, and review of transactions
 - 9.4 Administration of SAFE™ CMS Station – smart card functions
 - 9.5 Administration of SAFE™ CMS Server – smart card functions
 - 9.6 Administration of SAFE™ databases – schema review, backup and hot switching
 - 9.7 Administration of system logs – review and archiving
- 10. **SAFE™ System-to-System Server** – The server that performs the following functions:
 - 10.1 Registration of SAFE™ Payment Servers in individual domains
 - 10.2 Communication with other SAFE™ Communication Servers in other domains (system-to-system communications)
 - 10.3 Communication with external Servers of various Financial Services Providers (Remittance Providers, Bill Payments Providers, Currency Conversion Providers, etc.)
 - 10.4 Receiving and storing system-to-system transaction messages (outgoing messages)
 - 10.5 Receiving inquiries and sending system-to-system transaction messages (incoming messages)
- 11. **SAFE™ m-Phone Agent Application** – The application loaded in a mobile phone that supports SAFE™ agent functions:
 - 11.1 Registration of users
 - 11.2 Authorization of transactions
 - 11.3 Request for issuance of SAFE™ smart cards
- 12. **SAFE™ m-Phone Merchant Application** – The application loaded in a mobile phone that supports SAFE™ merchant functions:
 - 12.1 Registration of merchants
 - 12.2 Registration of merchant's location
 - 12.3 Payment transactions
 - 12.4 Acceptance of m-tickets, m-coupons, etc.
- 13. **SAFE™ PoS Merchant Application** – The application loaded in Point-of-Sale (PoS) devices supporting Over-the-Counter (OTC) payment transactions that performs the following functions:
 - 13.1 SAFE™ cash-in / cash-out transactions using SAFE™ smart cards, SAFE™ NFC Wallet or SAFE™ EMV cards
 - 13.2 Payments over-the-counter (OTC) using SAFE™ smart cards, SAFE™ NFC Wallet or SAFE™ EMV cards
 - 13.3 EMV transactions – OTC payments or ATM cash-out transactions using SAFE™ smart cards, SAFE™ NFC Wallet or SAFE™ EMV cards

- 14. SAFE™ PC Merchants Application** – The PC application supporting SAFE™ transactions using desktop Smart Card Reader (SCR), contact or contactless, that performs the following functions:
- 14.1 Cash-in / Cash-out using SAFE™ smart cards or SAFE™ NFC Wallet
 - 14.2 Payments over-the-counter using SAFE™ smart cards or SAFE™ NFC Wallet
 - 14.3 PIN and fingerprint authentication
- 15. SAFE™ m-Phone Wallet** – The application loaded in a mobile phone that performs the following functions:
- 15.1 User login using PIN
 - 15.2 Mobile financial transactions for banked users (m-Banking)
 - 15.3 Mobile financial transactions for un-banked users (m-Commerce)
 - 15.4 Merchant-to-distributor, merchant-to-merchant or any business-to-business payments
 - 15.5 Customer-to-merchant payments over-the-counter
- 16. SAFE™ UICC Wallet** – The application loaded in an User Integrated Circuit Chip (UICC) that performs the following functions:
- 16.1 Registration of users using mobile phones
 - 16.2 User login using PIN
 - 16.3 Mobile financial transactions for banked users (m-Banking)
 - 16.4 Mobile financial transactions for un-banked users (m-Commerce)
 - 16.5 Various types of payments transactions (person-to-person, person-to-merchant, business-to-business, etc.)
 - 16.6 Various security-setting functions
- 17. SAFE™ SIM Wallet** – The application loaded in a Subscriber Identity Module (SIM) chip that performs the following functions:
- 17.1 Registration of users using mobile phones
 - 17.2 User login using PIN
 - 17.3 Mobile financial transactions for banked users (m-Banking)
 - 17.4 Mobile financial transactions for un-banked users (m-Commerce)
 - 17.5 Various types of payments transactions (person-to-person, person-to-merchant, business-to-business, etc.)
 - 17.6 Various security-setting functions
- 18. SAFE™ NFC m-Phone Wallet** – The application loaded in a NFC-enabled mobile phone that performs the following functions:
- 18.1 Registration of users using mobile phones
 - 18.2 User login using PIN
 - 18.3 Mobile financial transactions for banked users (m-Banking)
 - 18.4 Mobile financial transactions for un-banked users (m-Commerce)
 - 18.5 Various types of payments transactions (person-to-person, person-to-merchant, business-to-business, etc.)
 - 18.6 Merchant-to-distributor NFC payments (OTC)
 - 18.7 Customer-to-merchant NFC payments (OTC)
- 19. SAFE™ NFC SD Card Wallet** – The application loaded in a NFC-enabled microSD card that performs the following functions:
- 19.1 Registration of users using mobile phones
 - 19.2 User login using PIN
 - 19.3 Mobile financial transactions for banked users (m-Banking)
 - 19.4 Mobile financial transactions for un-banked users (m-Commerce)
 - 19.5 Various types of payments transactions (person-to-person, person-to-merchant, business-to-business, etc.)
 - 19.6 Merchant-to-distributor NFC payments (OTC)
 - 19.7 Customer-to-merchant NFC payments (OTC)
- 20. SAFE™ NFC UICC Wallet** – The application loaded in a NFC-enabled User Integrated Circuit Chip (UICC) that performs the following functions:

- 20.1 Registration of users using mobile phones
- 20.2 User login using PIN
- 20.3 Mobile financial transactions for banked users (m-Banking)
- 20.4 Mobile financial transactions for un-banked users (m-Commerce)
- 20.5 Various types of payments transactions (person-to-person, person-to-merchant, business-to-business, etc.)
- 20.6 Merchant-to-distributor NFC payments (OTC)
- 20.7 Customer-to-merchant NFC payments (OTC)

21. **SAFE™ Web Payment Module** – The module combined with Web cash-out pages that enables SAFE™ customers to pay Web purchases using SAFE™ mobile accounts

B.1.2 SETECS® Mobile Services

For all its products, SETECS® Mobile will also provide back-end services to [Partner] to install, maintain, upgrade, and operate the products. Services to be provided by SETECS® Mobile will be classified in three groups – software services, security services, and operational services.

B.1.2.1 Software Licensing

- Distribution of SW on CDs for Servers and Stations
- Distribution of SW preloaded in PoS devices
- Downloading of Secure Mobile Wallet as m-Phone application
- Distribution of Secure Mobile Wallet as an applet in the SAFE™ smart card
- Distribution of Secure Mobile Wallet as a Wiblet preloaded in the SIM chip
- Static (OTC) and dynamic (OTA) loading and maintenance of Secure Mobile Wallet

B.1.2.2 Software Services

Software services are related to potential extensions of software, correctness of software, upgrades, maintenance, and protection of software. These services are the following:

- Analysis and approval of user requirements
- Correction of bugs
- Software upgrades and extensions
- Validation and verification of all external software modules
- Encryption of software modules

B.1.2.3 Security Services

Security services are related to registration, authentication, authorization, data and messages protection, and privacy procedures. These services are the following:

- Registration of participants – subscribers and companies
- Privacy and data protection
- Application messages and protocols messages security
- Key management operations
- Certificates and PKI management
- Authentication components and procedures
- Authorization policies – definition and enforcement
- Backup and archiving of data and system software

B.1.2.4 Operational Services

Operational services include all operations that are necessary and all prerequisite activities for normal, correct, secure and continuous mobile financial services. Operational services include:

- Support to enrollment and issuance of SAFE™ smart cards
- Issuance of X.509 certificates
- Selection and approval of hardware components used with the SAFE™ system
- Continuous and reliable operation of SAFE™ servers
- Installation, configuration, and activation of all SAFE™ components
- Installation of software upgrades

B.1.2.5 Communication Services

Communication services include sending message from the SAFE™ system to users (so called Mobile Terminating – MT messages) and from users to the SAFE™ system (so called Mobile Originating – MO messages). These services may be based on different communication protocols. SETECS® Mobile will provide communication services based on SMS messages. [Partner] will provide services based on GPRS or MMS messages. Communication services based on SMS messages include:

- Customization of the SAFE™ Communication Server to connect to the SMS Gateway of the aggregator
- Sending message from the SAFE™ system to users
- Receiving SMS messages from users
- Synchronization of system audit logs between SAFE™ Communication Server and SMS Gateway Server
- Automatic handling of connections in terms of disruptions
- Dynamic switching to alternative configurations in case of communication problems

B.2 [Partner]

[Partner] will be responsible for all software and hardware prerequisites, and for mobile financial services to be offered to system agents, merchants, and customers.

B.2.1 Software and Hardware Prerequisites

[Partner] will be responsible for availability and correct functioning of the following software and hardware prerequisites, as needed:

- **Communication Network – Connection to Telecoms**
 1. Communications of GPRS messages
 2. Communications of MMS messages
- **Connection and Use of GPRS and MMS Gateways**
 1. Receiving (bulk) incoming messages
 2. Sending (bulk) outgoing messages
 3. Sending MMS messages
- **Internet Connection**
 1. Standard Internet connection services
- **PoS Devices**
 1. Contact SC reader and support for contact SC protocol based on ISO 7816
 2. Contactless SC reader and support for contactless SC protocol based on ISO 14443
 3. Communication capabilities

B.2.2. Mobile Financial Services

[Partner] will provide the following mobile services to **system agents**:

- Registration of merchants and subscribers for mobile transactions;
- Opening merchants' and customers' SAFE™ mobile accounts;
- Enroll merchants and customers for issuance of SAFE™ smart cards
- Assist and support review of their financial transactions

[Partner] will provide the following mobile services to **merchants** registered in the SAFE™ system:

- Registration of merchants both for OTC and OTA financial transactions and as agents of the system (supporting OTC and OTA deposits to customers' SAFE™ mobile accounts);
- Opening and managing of their SAFE™ mobile accounts;
- Accepting cash as deposits to customers' SAFE™ mobile accounts (cash-in);
- Distributing cash to SAFE™ customers over-the-counter (cash-out);
- Accepting OTC and OTA financial transactions using SAFE™ smart cards or mobile phones for authentication of customers and security of transactions;
- Performing clearing of transactions (batch or individual) with the SAFE™ Payment Server and with back-end banks' servers managing their bank accounts;
- Review the status and individual transactions on their SAFE™ mobile accounts.

[Partner] will provide the following mobile services to **consumers** (mobile subscribers or card holders) and **banking customers**:

- Registration of customers as either card holders or mobile subscribers
- Initial loading of their SAFE™ Mobile Wallets into their mobile phones or issuance of their biometrics SAFE™ smart cards;
- Opening and managing of their SAFE™ mobile accounts associated with mobile phones or cards;
- Loading (pre-pay) money into their SAFE™ mobile accounts using on-line banking transfers, direct cash deposits (cash-in with SAFE™ merchants) or other classical money transfer mechanisms (credit/debit cards, international remittance transfers, cashing checks, direct deposits, etc);
- Using their mobile phones or smart cards for authentication to the SAFE™ Payment Server and for authorized manipulation with SAFE™ mobile accounts;
- Re-loading SAFE™ mobile accounts from bank accounts and returning pre-loaded amounts back to their corresponding bank accounts;
- Review the status and individual transactions on their SAFE™ mobile accounts.