

S.K.A.L.A. (SON KULLANICI ANALİZ ARACI) KULLANICI SÖZLEŞMESİ
S.K.A.L.A. (END USER ANALYSIS TOOL) USER AGREEMENT

I-Taraflar:

İşbu Sözleşme Kuveyt Türk Katılım Bankası A.Ş. (bundan sonra Banka olarak anılacaktır) ile Sözleşmeyi Banka tarafından sunulan elektronik ortam, platform, yazılım ya da uygulamalar üzerinden onaylayarak Sözleşme hükümlerini kabul eden Banka müşterisi (bundan sonra Müşteri olarak anılacaktır) arasında akdedilmiştir.

II-SKALA Hakkında Bilgilendirme

1) SKALA, Prodaft Siber Güvenlik Teknolojileri A.Ş. (bundan böyle kısaca "Firma" olarak anılacaktır) tarafından geliştirilmiş olan ve kullanıcılara anılan Firma tarafından sunulur, işletilmesi, yönetilmesi, bakım ve onarımı Firma tarafından sağlanan bir güvenlik yazılımıdır.

2) Firma, SKALA ile kullanıcıların telefon, tablet, dizüstü bilgisayar veya masaüstü bilgisayar gibi bankacılık ürün ve hizmetlerini kullandığı cihazlarında (bundan sonra Cihaz olarak anılacaktır), banka hesaplarına ya da bankacılıkla ilgili verilerine yetkisiz kişilerin erişimine sebep olabilecek ve dolayısıyla maddi kayıplarına yol açabilecek zararlı yazılımlar bulunup bulunmadığını anlık olarak tespit ederek, Bankaya bildirmektedir.

3) Firma, SKALA yazılımının yüklendiği Cihazları, SKALA vasıtasıyla tarayarak Cihazdaki zararlı yazılım içeren uygulamaları tespit etmekte ve bunları Banka'ya bildirmektedir. Banka da Firma'dan iletilen bu zararlı yazılım bildirimini Müşteriye iletecek ve Müşterinin internet ya da mobil bankacılık uygulamalarının bu zararlı yazılımdan etkilenmemesi için önlem almasını isteyecektir. Müşteri bu bildirim sonrası internet ya da mobil bankacılık uygulamalarının güvenliği için her türlü önlemi almayı kabul etmiştir. Bu şekilde bir zararlı yazılım bildirimi yapılması halinde Banka, Müşterinin mobil şube, mobil bankacılık ve internet bankacılığı kanallarını işleme kapatabilecektir.

4) Firma, SKALA aracılığıyla Müşterinin mobil bankacılık uygulamalarını kullandığı android tabanlı telefon ya da tabletlerinde, Cihaza yüklü bütün uygulamaların isim bilgilerini; IOS tabanlı telefon ve tabletlerinde ise Cihazın jailbreak (root) yapıp yapılmadığı (diğer ifadeyle Cihazın normal yapısında bir bozulma olup olmadığı) gibi genel bilgilerini; dizüstü ya da masaüstü bilgisayarlar ve sair elektronik cihazlar üzerinden internet bankacılığı uygulamalarını kullanan müşterilerin ise sessionID ve clientIP bilgilerini kendi sistemlerine bu Sözleşme hükümlerine göre inceleyerek, Cihaz içinde zararlı yazılım olup olmadığını tespiti çalışacaktır.

I-The Parties:

This agreement has been entered into by and between Kuveyt Türk Katılım Bankası A.Ş. (hereinafter referred to as the "Bank") and the Bank's customer who accepted the conditions set forth herein by approving this Agreement on an electronic platform, software program or application provided by the Bank (hereinafter referred to as the "Customer").

II-Information about SKALA

1) SKALA is a security software program developed by Prodaft Siber Güvenlik Teknolojileri A.Ş. (hereinafter referred to as the "Company"), provided by the Company to users, and operated, managed, maintained and repaired by the Company.

2) By using SKALA, the Company detects in real time whether or not a telephone set, tablet, laptop computer or personal computer (hereinafter referred to as the "Devices") by means of which a user uses any product or service of the Bank contains any malware that may enable an unauthorized person to gain access to that user's bank accounts or banking data and that may cause the user to suffer any material loss, and reports its finding to the Bank.

3) By using SCALA, the Company scans the Devices in which SKALA was installed, detects the malware installed in them, and notifies those malware to the Bank. The Bank will receive a malware notice from the Company, send that notice to the Customer, and ask the Customer to take precautions to prevent his/her online or mobile banking applications from being affected from that malware. The Customer agrees to take all kinds of precaution to secure his/her online or mobile banking applications after receiving such malware notice. In case the Bank sends such malware notice to the Customer, the Bank will be entitled to suspend the mobile branch, mobile banking and online banking channels of the Customer.

4) By using SKALA, the Bank will check the name details of all the applications installed in the Customer's Android-based telephone set or tablet, or whether the Customer's IOS-based telephone set or tablet has been made jailbreak (root) (i.e. whether or not the normal structure of the Device has broken down in any way), or the sessionID and clientIP data of the Customer's laptop or personal computer or other electronic device, through which the Customer uses mobile banking applications, in accordance with the terms specified in this Agreement, and



III-Kullanıma Dair Şartlar

İşbu Sözleşmenin onaylanması halinde SKALA'nın kullanımına ilişkin olarak aşağıdaki şartlar Müşteri tarafından kabul edilmiş olacaktır:

1) Müşteri bu Sözleşmeyi onaylayarak SKALA'nın Cihazına yüklenmesini kabul etmektedir. Sözleşmenin onaylanmasından sonra Müşterinin kullandığı mobil ya da internet bankacılığı uygulamasına ve dolayısıyla Müşterinin anılan uygulamaların kurulu bulunduğu Cihazlarına SKALA yüklenecektir.

2) Müşteri IOS ya da Android 8.1 ve sonrası versiyonlarının yüklü olduğu Cihazlar kullanıyorsa; mobil ya da internet bankacılığını kullanmaya başladığı anda SKALA programı, Cihazları tarayacak ve Müşterinin android tabanlı Cihazlarında, Cihaza yüklü bütün uygulamaların isim bilgilerini; IOS tabanlı Cihazlarda, Cihazın jailbreak(root) yapılıp yapılmadığı (diğer ifadeyle Cihazın normal yapısında bir bozulma olup olmadığı) gibi genel bilgilerini; dizüstü ya da masaüstü bilgisayarlar ve sair elektronik Cihazlarda ise Müşterinin ve Cihazın sessionID ve clientIP bilgilerini alarak, elektronik platformlar üzerinden Banka'ya iletecektir. Müşterinin Cihazlarında Android 8.0 ve öncesi versiyonlar yüklüyse, SKALA programı bankanın sunduğu mobil ve internet bankacılığı uygulamaları kapalıyken de yukarıda zikredilen taramaları yapacak ve Banka'ya yine yer alan bilgileri iletecektir.

3) Banka, SKALA programı tarafından kendisine iletilen bu verileri, bunlar üzerinde herhangi bir işlem ya da kontrol gerçekleştirmeksizin Firma sistemlerine aktaracaktır.

4) Firma, SKALA tarafından yapılan tarama sonucu alınan verileri inceleyecektir. Bu inceleme sonucunda Cihaz içinde Müşterinin banka hesaplarına ilişkin bilgilerin yetkisiz üçüncü kişilerin eline geçmesine neden olabilecek zararlı yazılımlar tespit etmesi halinde Firma, bu durumu Bankaya bildirecektir. Banka da, bu bildirimde istinaden Müşteriye zararlı yazılım bildiriminde bulunacaktır. Müşteri bu bildirim üzerine cihazının sıfırlanması da dahil olmak üzere Cihazının güvenliği için gerekli önlemleri almakla yükümlüdür. Bu şekilde bir zararlı yazılım bildirimi yapılması halinde Banka, Müşterinin mobil şube, mobil bankacılık ve internet bankacılığı kanallarını işleme kapatma yetkisini haizdir. Müşteri, Banka'nın bu yetkisini kullanmasına itiraz etmeyeceğini kabul ve taahhüt etmiştir. Müşteri, anılan mobil ve internet bankacılığı kanallarının tekrar açılması için Bankaya müracaat hakkına sahiptir.

5) Müşteri, bu Sözleşmeyi onaylamakla, SKALA programının, Cihazlarında yukarıda anılan tarama işlemlerini gerçekleştirmesini, tarama sonucu tespit ettiği uygulama ismi, jailbreak bulguları, sessionID ve clientIP bilgileri gibi, programın zararlı yazılım tespit fonksiyonunu ifa edebilmesi için gerekli bilgi ve bulguların Banka sistemlerine ve Banka tarafından da Firma'ya aktarılmasını talep ve kabul etmektedir.

the Bank will try to find out whether the Device contains any malware.

III-Conditions of Use

If the Customer approves this Agreement, he/she will be considered to have accepted the conditions described below and governing the use of SKALA:

1) The Customer agrees the installation of SKALA in his/her Device by approving this Agreement. After this Agreement has been approved, SKALA will be installed in the mobile or online banking application used by the Customer and, consequently, in the Customer's Device in which the said application was installed.

2) If the Customer uses a Device running on IOS or Android 8.1 or later, SCALA will scan the Device the moment the Customer has started to use his/her mobile or online banking application and will check the name details of all the applications installed in the Customer's Android-based telephone set or tablet, or whether the Customer's IOS-based telephone set or tablet has been made jailbreak (root) (i.e. whether or not the normal structure of the Device has broken down in any way), or the sessionID and clientIP data of the Customer's laptop or personal computer or other electronic device, and send those data to the Bank through an electronic platform.

If the Customer's Device runs on Android 8.0 or an earlier version thereof, SCALA will perform the scans described above even when the Customer's mobile or online banking application is turned off, and send those data to the Bank.

3) The Bank will receive the above mentioned data from SKALA and send them to the Company's system without processing or checking them in any way.

4) The Company will check the data it has received from SKALA after the said checks have been performed. If the Company finds out that the Device contains a malware which may enable an unauthorized third party person to gain access to the Customer's bank account details, the Company will notify the situation to the Bank. Upon receiving such notice, the Bank will send a malware notice to the Customer. Upon receiving such malware notice, the Customer will be obliged to take the precautions needed to secure his/her Device including resetting his/her Device. In case the Bank sends such malware notice to the Customer, the Bank will be entitled to suspend the mobile branch, mobile banking and online banking channels of the Customer. The Customer agrees and undertakes not to object the Bank's use of its above mentioned authorization. The Customer has the right to apply to the Bank for reactivation of his/her suspended mobile branch, mobile banking and online banking channels.

5) By approving this Agreement, the Customer asks and agrees the SCALA application to perform the scan described above in his/her Devices and to transfer the resulting application name, jailbreak findings, sessionID,



6) Firma, SKALA programının etkin işleyebilmesi için program üzerinden kendisine aktarılan bu verileri kendi sistemlerinde işleyebilecek, muhtemel zararlı yazılım bilgileri ile karşılaştırabilecek, bunların yedeklerini alabilecek ve bunları saklayabilecektir. Müşteri Banka ve Firma'nın anılan bilgi veya verileri bu şekilde işlemesine, saklamasına ve birbirine aktarmasına muvafakat etmektedir.

7) SKALA, zararlı yazılımın Cihaza yüklenmesini önleyen bir program veya yazılım değildir. Müşteri Cihazında SKALA yüklenmiş olması, Cihazın zararlı yazılımlardan korunacağı anlamına gelmeyecektir. Bu nedenle Müşteri, Cihazına zararlı yazılımlar yüklenmemesi için gerekli önlemleri almaktan bizzat sorumludur. Bu anlamda Müşteri, kaynağı belirsiz internet sitelerine girmemek, tanımadığı kişi, kurum ya da kaynaklardan kendisine gönderilen bildirim, bilgi talebi, üyelik daveti, ücretsiz ya da düşük meblağlı mal ya da hizmet satışları, hediye, promosyon vaadlerini kabul etmemek, bunları onaylamamak ya da bunlarla iletişim kurmamak, kumar, bahis, porno içerikli siteler gibi yasadışı içerik ya da uygulamalara girişler yapmamak ve sair zararlı yazılımların yüklenmesine yol açabilecek işlemlerden uzak durmakla yükümlüdür.

8) Cihazın gerek fiziki ve gerekse yazılım açılarından her türlü güvenliğinin sağlanmasından, virüs, trojan gibi zararlı unsurlardan korunmasından münhasıran Müşteri sorumludur. Müşteri, Cihazının ve bankacılık uygulamalarının herhangi bir üçüncü kişinin eline geçmemesi ya da erişimine açılmaması için tüm güvenlik tedbirlerini almaya devam edecektir. Müşteri, Banka tarafından kendisine verilmiş olan şifre, parola gibi bankacılık uygulamalarına giriş ya da güvenlik bilgilerini, yine kendisine ait kimlik bilgilerini, kişisel verilerini ve sair bilgileri üçüncü kişilerle paylaşmayacaktır. SKALA'nın Müşterinin Cihazına yüklenmiş olması, Müşterinin yukarıda anılan yükümlülüklerinin sona erdiği ya da azaldığı anlamına gelmeyecektir.

9) SKALA, Müşterinin Cihazındaki banka hesapları ya da bankacılık uygulamalarına ilişkin her türlü zararlı yazılımı tespit etme garantisi sunmamaktadır. Dolayısıyla SKALA'nın Cihaza yüklenmiş olması, Cihazdaki müşteri hesap bilgileri ya da bankacılık uygulamalarına ilişkin her türlü zararlı yazılımın tespit edilebileceği anlamına gelmemektedir. Müşteri Cihazının korunması için gerekli güvenlik önlemlerine riayet etmezse, Cihazına zararlı yazılım yüklenebilecek ve hesap bilgileri üçüncü kişilerin eline geçebilecektir. Bu tür durumlarda yetkisiz ve kötü niyetli üçüncü kişiler Müşteri hesaplarındaki nakit, kıymetli maden ya da menkul kıymetleri başka hesaplara transfer ederek Müşterinin maddi kayıplara uğramasına neden olabilecektir. Bu nedenle SKALA'nın yüklenmiş olmasına rağmen Müşterinin Cihazında zararlı yazılımlar bulunması

clientID, and the information and findings it needs to perform its function to detect malware to the Bank's systems, and the Customer asks and agrees the Bank to transfer the said data to the Company.

6) The Company may process the data transferred by SCALA to its system, compare them with possible malware data, back them up, and store them to ensure SKALA to run in an efficient way. The Customer permits the Bank and the Company to process, store and transfer the above mentioned information and data as described above.

7) SKALA is not a program or software that prevents malware from being installed in the Device. The fact that SCALA was installed in the Customer's Device will not mean that the Device will be protected from malware. Therefore the Customer is responsible for taking the precautions needed to prevent malware from being installed in his/her Device. For this purpose the Customer is obliged not to visit websites of unknown origin; not to accept, approve or communicate with regard to any notice, request for information, invitation to register as a member, offer to buy any product or service free of charge or at a low price, gift or promotions; not to visit any website containing such illegal contents or applications as gamble, betting or pornography, and to keep away from steps that may install any malware in his/her Device.

8) The Customer is exclusively responsible for taking all kinds of security measure in both physical and software terms for his/her Device and for protecting his/her Device from such malicious things as viruses, trojans, etc. The Customer will keep on taking the security measures needed to prevent his/her Device and banking applications from being captured or accessed by third parties. The Customer will not disclose such banking application log-in or security information allocated to him/her by the Bank and his/her identity details, personal data and similar information to third parties. The fact that SKALA was installed in the Customer's Device will not mean that the above mentioned obligations of the Customers have ended or decreased.

9) SKALA does not guarantee to detect all kinds of malware in the bank accounts or banking applications installed in the Customer's Device. Therefore, the fact that SKALA was installed in the Customer's Device will not mean that it will be able to detect all kinds of malware in the Customer's bank account details or banking applications. If the Customer fails to take the measures necessary to protect his/her Device, some malware may install itself in his/her Device and his/her account details may be captured by third parties. In this case an unauthorized and malicious third party may transfer some cash, precious metal or securities from the Customer's accounts to other accounts and cause the Customer to suffer a material loss. Therefore, the Customer will be exclusively liable for the losses he/she may suffer because of a malware installed in his/her Device



ve bunun tespit edilmemiş olması hallerinde de Müşterinin maruz kalacağı zararlarından sadece Müşteri sorumludur. Müşteri bu nedenlerle Banka ya da Firmanın bir sorumluluğu bulunmayacağını kabul etmiştir.

10) SKALA sadece mobil ya da internet bankacılığı sistemlerine yetkisiz erişime neden olabilecek zararlı yazılımları taramak amacıyla geliştirilmiş bir yazılımdır; bu nedenle Müşteri Cihazındaki diğer zararlı yazılımları taramayacak, tespit etmeyecek ve bildirmeyecektir.

11) SKALA'nın yazılım ve kullanım haklarına ilişkin her türlü sorumluluk Firma'ya aittir. SKALA'nın Müşterinin Cihazında neden olacağı sorun ve zararlardan da Firma sorumlu olacaktır. Müşteri bu kapsamda Banka'dan bir talepte bulunmayacağını kabul etmiştir.

12) Firma, zaman zaman SKALA üzerinde bakım, onarım ve güncelleştirme çalışmaları yapabilecek olup, bu anlarda SKALA'nın çalışmaması söz konusu olabilecektir. Yine SKALA'nın Müşterinin Cihazlarına uyumlu olacağına dair bir garanti de verilememekte olup, Müşteri Cihazındaki teknik özellikler nedeniyle SKALA'nın çalışmamasından dolayı Banka ya da Firmanın sorumluluğu olmayacaktır.

IV-SKALA Kullanma İzni

SKALA, Firma'ya ait bir yazılım olup, Firma ile Banka arasında akdedilen sözleşmeler uyarınca bu yazılımın kullanma izni Banka'ya verilmiştir. Banka da bu izne istinaden SKALA'ya kendi Müşterilerine kullandırmaktadır. Buna göre SKALA sadece Müşterinin Cihazındaki Banka'nın sunduğu internet ya da mobil bankacılık uygulamasının bir eklentisi olarak kullanılabilir.

Bu Sözleşme Müşteriye, SKALA üzerinde herhangi bir fikri ya da sınai mülkiyet hakkı veya bu kapsamda bir mali ya da manevi hak verildiği anlamına gelmemektedir. Müşterinin SKALA üzerinde hiçbir hak ve yetkisi bulunmamaktadır.

V-Bankacılık Hizmetleri Sözleşmesi ile Bağlantı

İşbu Sözleşme, Banka ile Müşteri arasındaki Bankacılık Hizmetleri Sözleşmesi (BHS)'nin eki ve ayrılmaz bir parçası hükmünde olup, bu Sözleşmede düzenlenmeyen her konuda BHS hükümleri uygulanacaktır.

VI-Sözleşmenin Süresi ve Sona Ermesi

Müşteri SKALA'yı işbu Sözleşmenin yürürlükte kaldığı sürece kullanabilecek olup herhangi bir nedenle bu Sözleşmenin ya da BHS'nin sona ermesi halinde SKALA programı da kullanılamayacaktır.

and not detected by SCALA despite the fact that SKALA was installed in his/her Device. The Customer agrees that neither the Bank nor the Company may be held liable for such loss.

10) SKALA is a software program developed only for the purpose of scanning malware which may lead to unauthorized access to mobile or online banking systems; therefore it will neither scan, nor detect, nor report any other malware in the Customer's Device.

11) All kinds of responsibility for the software and utilization rights of SKALA remains with the Company. The Company will also be responsible for problems and damages which SCALA may cause the Customer's Device to suffer. The Customer agrees not to claim anything from the Bank with regard to such problem or damage.

12) The Company may perform maintenance, repair or update work on SCALA time to time, so that SKALA may not run during such work. It is not guaranteed that SCALA will support the Customer's Device, so that neither the Bank nor the Company will be responsible for SCALA's failure to run because of the technical properties of the Customer's Device.

IV-License to use SKALA

SCALA is a software program owned by the Company, and the Company has licensed the Bank to use it under the agreements entered into by and between the Company and the Bank. The Bank permits its customers to use SCALA under the above mentioned license. Therefore SCALA may be used only as part of the online or mobile banking application installed by the Bank in the Customer's Device. This Agreement does not grant the Customer any intellectual or industrial property right, any financial right or any moral right of SCALA. The Customer holds no right or power whatsoever on SCALA.

V-Relation with the Banking Services Agreement

This Agreement is an annex and integral part to the Banking Services Agreement (BHS), and the matters not specified in this Agreement will be subject to the conditions set out in the BHS.

VI-Term and Termination

The Customer will be allowed to use SCALA as long as this Agreement remains valid, and not be entitled to use SCALA if this Agreement or the BHS is terminated due to any reason.

Müşteri / Customer:

ONAYLIYORUM. / APPROVED.

