Cardinal
Számítástechnikai Kft.
1025 Budapest, Pusztaszeri út 91. +36 1 345 7980 http://www.cardinal.hu

Introduction to ViCA Application

(ViCA 2.0)

Version: 1.0

May 2020

Content

1. Summary

ViCA (Virtual Chipcard Application) is an innovative mobile authentication tool of Cardinal Ltd., which supports the legal regulation of two-factor based, Strong Customer Authentication procedure (SCA) required by the Regulatory Technical Standard of European Banking Authority (EBA-RTS) in the European Union's PSD2 Directive. The application is available on Android, iOS and Windows platforms.

Mobile phone – as a tool for personal identification

With the development of the Virtual Smart Card Application (ViCA), Cardinal has set itself the goal of **making mobile phone a personal authentication tool**. The application enables **two-factor (2FA)** (based on RSA, PKI technology) **user authentication**. ViCA is password protected and can be installed on a mobile device or desktop computer running Windows.

With the help of ViCA, the installed Electra Client Program, Electra Internet Banking and Mobile Banking user interfaces, as well as Electra Mobile App application **generate signing key pairs and certificates with which it can be registered for the use of the Electra system**. Using the certificate, users can securely log in to Electra applications and sign and authenticate their orders recorded on client interfaces electronically.

Compared to a chipcard, the ViCA application can also be used for authentication when the user uses the bank's services from a mobile phone or tablet in the same time. **The SMS code** contains only a one-time password ford authentication, while ViCA signs orders with the user's own private key. **With the QR code** authentication and authorization procedure, the use of ViCA is more convenient for the users. It can be used to perform the desired authentication operation faster, thus also providing an enhanced user experience. ViCA provides the possibility to show individual transaction data when signing orders (dynamic linking as a PSD2 EBA-RTS standard). This isn't available when using QR code.

The application works with standard and easily auditable tools and algorithms (RSA, SSL, PBKDF2).

Two-factor verification - 2FA

Multi-factor authentication is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: **knowledge** (something that is only known by the user), **possession** (something that is only the user has), and **inherence** (something that is only the user is).

ViCA app employs a two-factor authentication, which is a subset of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors: **i) something they know, ii) something they have, or iii) something they are.**

Biometric identification

Inherence factors – mentioned above – include any biological traits the user has that are confirmed for log in. This category includes the scope of biometrics such as retina scans, iris scans, fingerprint scans, facial recognition, voice recognition, etc. By using the built-in biometric authentication methods of mobile devices running Android and iOS operating systems **ViCA app provides the fingerprint scans as biometric identification** (as for the 2nd factor of the authentication). By choosing this method of authentication, it is no more need to enter the ViCA password when starting the application, instead you can use the secure biometric identification provided by the given device and operating system.

Two-channel communication

One of the greatest strengths of the ViCA application is that it **opens a separate communication channel to the bank**, regardless of the channel used by Internet- or Mobile Banking. Thus, the connection between the ViCA application and the bank **remains secure even in the event of a hacker attack** targeting the Internet- or Mobile Banking connection.

In addition to the **use of public key infrastructure (PKI)**, the two-channel authentication further enhances user security. Using ViCA, you don't need passwords or token codes, which can be obtained through a **phishing attack**.

The application provides the possibility to detect the man in the middle (**pharming**) attacks, too.

Dynamic linking

The use of the application supports the fulfilment of the "dynamic linking" regulation defined in the PSD2 Directive in the process of approval and authorisation of transactions to be submitted to the bank.

ViCA Micro Server

The broader applicability of the strong authentication procedure forced by the PSD2 Directive is ensured by the stand-alone server version of the application: The ViCA Micro Server.

This allows banks to use the application supporting the strong authentication method of the PSD2 Directive not only in a closed system - the Electra ecosystem - but for other third party service processing of the bank where the current legislation or the bank's internal regulation requires a strong customer authentication procedure.

With the implementation of ViCA Micro Server a special additional service becomes available, through which banks can messaging their clientele directly: **The Push Messaging (see later).**

One App with a multibank function

The ViCA app registered by a given user is linked to the user herself and not to a specific bank. This means that if the user uses the Electra system of several banks at the same time, she can register to all other banks with the once registered ViCA app.

By logging into the ViCA app, the user can keep the communication with the already registered banks while the app is running, so there is no need to constantly switch between the individual banks on the device while using several banking connections at the same time.

In ViCA app, messages from each bank are displayed on the screen of the device running the application according to the unique design of each bank.

Push messaging

ViCA is also capable of receiving messages from banks, which the bank can send from its own Electra system or from other back-end systems **via an appropriate API**. (e.g. bank account balance notifications, messages addressed to a targeted user for marketing purposes, product information, etc). Incoming messages are stored by ViCA in an encrypted form. The condition for providing the service requires the implementation of the ViCA Micro Server.

Cost-effectiveness

Using the ViCA application it **eliminates the cost of sending SMS** during the login process to the banking system as well as during the process of signing a specific transaction. By running the ViCA application on the user’s own device, the bank **doesn't have to procure and maintain additional supplies and infrastructure** (tokens, chipcards or card readers).

ViCA's Push Messaging Service allows the bank to forward banking information (e.g. transaction notifications, daily balance, warnings, bank product information, promotional campaign messages, etc) in a secure way, that is currently sent via SMS, **without additional costs to account holders**. This allows banks **to achieve significant cost savings**, as they can send various messages via ViCA instead of sending costly SMSes.

How to access the service provided by ViCA App?

The application cannot be used for internet banking on its own, it requires an existing Electra user interface. Its use is recorded by the bank on the basis of the contract concluded with the bank as the electronic channel(s) used by the user.

The app can be downloaded from **Google Play** for devices running Android, from the **App Store** for devices running Apple iOS, and from the **Microsoft Store** for Windows.

2. How it works

With the Virtual Chipcard Application (ViCA), mobile phones or the desktop computers become personal authentication devices. The application allows users of the Electra Client Program, Electra Internet- and Mobile Banking, as well as the Electra Mobile App channels to generate and register the key pairs (signing private and public keys) and certificates to use the Electra system. Customers /and the corporate users enabled by customers/ can use them to authorize their orders to their account servicing payment service provider in a secure way.

The **ViCA application** can be registered in the Electra system of several banks at the same time. It keeps in touch with all registered banks in parallel while the application is running. In this way, users shouldn't switch between various authentication tools between banks while in use. All messages from a bank are displayed on the screen according to the image of that bank.

On a security scale, the ViCA application itself ranks between SMS password and chipcard authentication. **ViCA is stronger and more cost-effective** than SMS password signing, while it is weaker than chipcard signing, but it **can be used much more broadly.**

Compared to a chipcard, ViCA application can also be used for authentication when the user uses the bank's services from a mobile phone or tablet at the same time.

The SMS code contains only a one-time password ford authentication, while ViCA signs orders with the user's own private key.

With the QR code authentication and authorization procedure, the use of ViCA is more convenient for the users. It can be used to perform the desired authentication procedure faster, thus also providing an enhanced user experience. ViCA provides the possibility **to show individual transaction data** when signing orders (dynamic linking as a PSD2 EBA-RTS standard). This isn't available when using QR code.

The application works with standard and easily auditable tools and algorithms (RSA, SSL, PBKDF2).

2.1 availability of the ViCA application

The ViCA application is uploaded by Cardinal Ltd. to the **App Store**, **Google Play** and the **Microsoft Store**, signed with its own developer certificate.

The ViCA app is available for mobiles and tablets running iOS 10+, Android 4.1+. Desktop ViCA is available for Windows win7 and win10 operating environments. The development for availability of later versions is ongoing.

2.2 technical prerequisites for the users

1. Using a **smartphone or a tablet**:
    - Android devices: requires Android 4.1 or later operating systems,

- iOS devices (iPhone – iPad – iPod touch): requires iOS 10.0 or later operating systems.

2. **For Desktop ViCA** (used on a desktop computer):
   - Windows win7 or win10 operating system.
3. **Reception capacity of ViCA registration password sent by the bank in an SMS** after the assignment of the ViCA application - as an authentication tool - to the user in the bank's own Admin interface.
4. **Internet connection** (mobile internet, WiFi or wired - in case of Desktop ViCA) on the device on which the application is installed for the registration of the application and its subsequent operation.

2.3 how to install the app

The app can be downloaded from **Google Play** for Android mobile devices, from the **App Store** for Apple iOS, and from the **Microsoft Store** for Windows.

When starting the application for the first time, the user must enter the **ViCA password**, which protects the app. You cannot start ViCA without knowing it.

For security reasons Cardinal Ltd. determines the requirements for it's structure (**in a pre-defined password policy**), and the structure is the same in all banks. It is a combination of (lowercase and uppercase) letters as well as numbers that should consist minimum of 8 and a maximum of 16 characters.

During its first setting the strength of the chosen password is shown graphically by the application in the user interface. The general password policy announced by Cardinal takes into account the strongest and most stringent policies of the banks using ViCA.

After registration done, the app can be started with this password solely.

2.4 certificate generation and registration

As a first step in the process, the account-holding bank must assign ViCA to the user as her authentication tool on the bank's own Electra Admin interface. The user then installs the application on the device from the Store according to the operating system of her own device. This is followed by registering the ViCA application via the ViCA app to the selected bank.

During the process the user generates a private and public keypair with the application. (The public and private keys are like two halves of a single key). To do this, you must enter your **Electra group code** (if there is any), **the short name** (or alias), and **the login password** in the application.

Based on this, the **account servicing provider will send an OTP code in a confirmation SMS to the mobile phone**, which number previously enrolled for ViCA registration, which you must enter in the field provided on the registration screen.

The confirmation code is a **time-limited one-time-password**, what connects the user ID and the ViCA application (and its running device, too).

The application then sends a standard Certificate Signing Request (CSR) to the Server in the format of Public Key Cryptography Standards (PKCS) #10. The Server creates a certificate from the public key signed with the Server's own secret key, and registers the PBKDF (Password-Based Key Derivation Function) code generated from the ViCA password into the Server.

Private keys and certificates created by ViCA are valid for a full year. One month before their expiry, the **ViCA application automatically renews the certificate.**

A prerequisite condition to register a certificate is the enrollment of the user to use ViCA in the banking Admin program by the bank. The certificate contains only data that is available on the phone. i.e. it doesn't contain any banking authentication data nor other sensitive information. (**In the worse case when the mobile phone is lost or stolen, you can't extract confidential data from**). After succeeded the registration, private key is stored on the device in an encrypted form.

One half of the key used for encryption is derived from the parameters of the device using the installed application, while the other half is stored by the Electra Server and is only passed to the application when the appropriate ViCA password is entered. After three failed entry attempt Electra Server will **block the user** /e.g. if you enter an incorrect password/. Without a proper device and an appropriate ViCA password, it is impossible to decrypt the private key.

ViCA password won't be ever stored in the ViCA app - neither in an encrypted form.

2.5 launching the app

To start the entry process the application asks for the ViCA password and then logs in to the banking Server with the certificate and ViCA password. In case the data sent to the bank when logging into ViCA is correct, Electra Server will return the Server key required to decrypt the previously registered private key.

The ViCA app doesn't store the ViCA password, its correctness is checked by the banking back-ends, so the ViCA password cannot be determined by systematic attempts either. After three consecutive ViCA password errors, the ViCA app access will be blocked in the bank's back-end. Following such an event, it is not possible to log in to the Server even if the correct password is entered.

The ViCA app protects the locally stored private key with an encryption key stored on the Server. Without the bank Server, the locally encrypted private key cannot be decrypted, however, the encrypted private key is not available on the bank Server.

Because the **application can be used in multiple banks**, password verification and bank records of corrupted passwords are performed according to a built-in algorithm in the order of frequency of use of registered banks.

2.6 multilateral registration of one single user

There ar banks, which make possible for a user to register on behalf of multiple banking clients. This is typically required when a private individual appears as more than one customer as a bank user. It is important that in this case the behind the "multiple bank user" stands the same private individual and the bank makes sure of this and identifies the user. This is possible in the Registration menu. All users are registered as described above. In case of registration with several banks, after the first registration no new key-pair (public and private) and certificate will be created during further registrations: **the signature will be made with the same certificate.**

2.7 using the app to login (authentication)

The application can be used to access the Internet Banking, the Electra Client Program, and the Mobile Banking as well as the Electra Mobile App interfaces for secure authentication of the user's identity.

During login process into the banking systems, the identification of the user can be initiated with the help of the user ID specified for the use of the given interface. When using Android, iOS, and Windows win7 and win10 applications, the device running ViCA receives a push notification from the Server informing the user that the ViCA application needs to be started.

The application uses the **private key and its associated certificate to perform** the actions required to complete **the login** to the Electra user interface(s). After that, the interface will automatically take you to the first page after logging-in of Electra Client Program and to the overview page of the Electra Internet Banking.

2.8 using the app to sign (authorization)

In the Electra Client Program, Internet and Mobile Banking, as well as in Mobile App, the user selects the packages she wants to sign (in case of immediate submission, she has successfully completed the correct entry of the order). The specific Electra client interface instructs the user to launch the ViCA application on the mobile device and select the appropriate function. (Applications running on Android, iOS and Windows win7 and win10 will also receive a push message).

The application displays the information **belonging to the signing user**: package names, beneficiary's account, the currency and the amounts of each order, the name of the signing user as well as the date of signing. Following the confirmation with entering the ViCA password the packages are signed. The Electra client interface automatically proceeds to the confirmation screen (signatures have been completed) and in case of immediate submission, the order is sent to the bank immediately.

In ViCA, the user has the **option to reject a signature initiated from the Electra client interface**. In this case, the Electra user interface displays a rejection warning message and the order packages assigned to signature remain unchanged.

In some banks – at the explicit request of the bank – for security reasons, the application also **asks for the ViCA password immediately before each signature**, which is verified when sent to the banking bank-ends.

2.9 biometric identification

In applications running Android and iOS operating systems, it is possible to switch to biometric identification after registration process. By using the built-in biometric authentication methods of mobile devices running Android and iOS operating systems **ViCA app provides the fingerprint scans as biometric identification** (as for the 2nd factor of the authentication). By selecting this, it is no more necessary to enter the ViCA password when starting the ViCA application after setting it up. Instead, secure biometric identification provided by the device and operating system can be used. For the Android version, this convenience feature can be turned on or off within the app itself. For iOS, biometric authentication can be turned on when ViCA is run for the first time or when a password is changed.

To use this service, the mobile device must possess a **fingerprint reader**.

2.10 password change

A **separate menu item can be used** in the application to change the ViCA password. Password change can only be performed if all registered bank Servers are available and support the password change function, as the changed password must be validated in all banks. If the exchange is successful on all affected bank Servers, the user will be notified and will only be able to use her application with a new ViCA password.

2.11 tracking the frequently used banks preferred by the user

The ViCA application **monitors which of the registered banks the user uses most often**, i.e. from which the most login and signing messages come. The application sorts the banks according to the number of messages and connects by default to the bank that the user uses most often.

Since the ViCA password is checked first by the first connected bank, it is possible to avoid the user being banned in a rarely used bank in case of password breakage, where - due to infrequent use - the user may have problems with the administration related to unlocking.

Based on the number of messages received, **the application recalculates the ranking of the banks once a week**, on the first use of the week.

2.12 ViCA push messaging

Deploying VMS in a banking environment allows you to access an additional feature of the ViCA application: sending and receiving and managing messages of different types and contents initiated from other banking processing and communication systems on customers' mobile devices. The service is **cost-effective, as banks can forward their targeted messages to individual users free of charge.**

The messages can be as follows:

- Balance of specific accounts,
- Transaction notifications,
- Orders not fulfilled or rejected,
- Request to Pay messages received,
- Access to new order packages waiting to be signed,
- Loan repayments due,
- Payment deadline warnings,
- Monitoring service configured to use the credit card or a bank account,
- Banking broadcasts,
- Personalized banking product offers, promotional campaigns, and
- Other messages.

Due to the implementation of VMS, **the application is capable of transmitting messages from systems other than the Electra system via a suitable API as well.**

Until the ViCA application won't be open on the user's mobile device, the phone will display a push notification on the user's device about the fact that a message has been sent to the ViCA application. It is important that the **push notification itself doesn't contain any personal or business information.**

Next time when the mobile application is opened, the user's ViCA application is connected to the VMS, from where the specific message, together with its entire content arrives on the user's mobile device **via an SSL-protected channel**.

Incoming messages are displayed on the touch screen in a transparent, tabular format according to their “subject”. If, in addition to the information sent in the "subject" field, the bank has also placed additional message content, clicking on the "subject" will display the entire content of the message **in a view in ViCA**. If the user closes the message after reading, she returns to the push notifications summary table.

ViCA's messaging service is language-dependent, that means if the "subject" has been sent in more than one language, **ViCA will recognize it and show the content in the language set by the application only** to the user.

The system **compiles statistics on ViCA messages** sent by the bank, which can be queried by the bank administrator in the WebAdmin interface according to the desired grouping. (Subject and content of ViCA message, status of the message, date of delivery to the recipient, time of SMS fallback, external ID).

The offered solution optionally provides the possibility of **fallback mechanisms**. Thus, the user can also receive the message via SMS if it hasn't been downloaded in the ViCA application for a certain period of time.

Optionally, a so-called "**SMS timer**" can be set, in which after a certain period of time the VMS sends an SMS content specified as a parameter to the mobile device of the user registered in the bank.

By setting the "**Message timer**", the expiration of the message can be limited in time until the sent ViCA message can be downloaded on the user's phone.

The „**External ID**" is the bank's own identifier that allows the re-pairing of bank messages (no appearence on the screen).

2.12.1 inquiry of sent notifications – new feature in Electra WebAdmin

In the Electra WebAdmin interface, the query of sent ViCA messages is **available to the bank as a separate function** regarding the following information:

- the subject and content of the ViCA message,
- message status,
- date of delivery to the addressee,
- SMS fallback time,
- external ID (the bank's own identifier that allows the re-pairing of bank messages).

The queried **content can be exported** from the application.

3. ViCA application architecture

The ViCA application opens **an independent TCP/IP channel protected by SSL encryption to the Electra Server and the ViCA Micro Server**. The IP address of the Electra Server as well as the ViCA Micro Server is encrypted by the application, which is signed with a developer key, so **the application is protected by the operating system against external, malicious manipulation**. There is a unique communication protocol (i.e. no HTTPS) between ViCA App and the Electra Server and the ViCA Micro Server, so it cannot be assaulted without the knowledge of the protocol, and the "usual" HTTP protocol attacks are ineffective.

Using the ViCA App it means literally that at the time of signing, the connection established in a channel is completely independent of the Electra channel between the ViCA application and the Electra Server or ViCA Micro Server. The authentication data

required for the signature is sent to the ViCA application by the Electra Server and the ViCA Micro Server on this separate channel.

4. ViCA Micro Server (VMS)

ViCA Micro Server is a stand-alone server that **manages all ViCA-related operations**. It manages its own database, in which it records the currently registered and pending users waiting for registration.

VMS serves ViCA applications running on iOS, Android, and Windows win7 and win10 operating platforms. Notifications and messages can be sent to these three platforms to individual users in a targeted way from banking back-end, and communication systems, as well.

In addition to serving the users of Electra channels by implementing the ViCA Micro Server in banking environment it provides the possibility for third party systems of the bank to use the services of ViCA through Web Service calls. Thus, the bank can manage either the **single users** applying the Electra channels or a separate **segment of users** completely independent of Electra with the same ViCA application. **Each clientele segment is managed separately by VMS.**

VMS can technically be run in two modes in the banking environment: **stand-alone** or **embedded**.

In the embedded mode, VMS is part of the Electra Server, which starts and stops together with the Electra Server, in which case there is no way to access Web Service, so only the Electra Server has control over the ViCA users (other banking processing systems don't).

4.1 ViCA Micro Server Web Service API

The ViCA Micro Server (VMS) Web Service API allows other banking back-end systems to send messages to users through the ViCA application as well.

In addition to the messaging function, external banking systems can also use ViCA authentication through the ViCA Micro Server service. If a banking system requires the use of strong customer authentication, a ViCA authentication process can be initiated or managed through this API.

Features provided by the API:

- ViCA messaging,
- starting user authentication,
- verification of signatures on user's orders,
- approval of ViCA registration,
- disable ViCA registration,
- inquiry of ViCA registrations,
- retrieve and filter messages.

5. Reference list

ViCA application is available to the clientele of the following banks: