**VU Security Mobile Tokens**

It is the first solution to provide a flexible scheme, easy to use, simple to implement and easy distribution all timely to introduce a dual-factor authentication. Used as hardware support cell phone customer. Thus end users have a guarantee that no person may intentionally capture their credentials and then use in a fraud or theft of banking information (phishing).

**What is a dual-factor authentication based on mobile devices?**

It is a multiplatform application with support for J2ME, iOS (Apple), Android, Blackberry, USSD and SMS generated password once. It works in conjunction with a server module to implement a secure authentication system, without direct connection between the user module and server module.

**Where is it installed?**

The VU Application Server module can be implemented in any technology environment because it is cross-platform and provides a broad integration capabilities; either through SOA, Radius or using APIs for custom integration. Created with large-scale environments in mind, the solution has a distributed architecture that allows scalability, high availability and fault tolerant system easily and safely. EI expertise of the development team VU Security allows integrating the solution in virtually any technology environment.

**How does it work?**

VU Security Mobile Token to generate a one-time password (OTP) on a cell phone, smartphone or mobile device support through each of the Markets. When the user needs to enter a system, uses the password (OTP) generated in your personal device and its static password, ensuring that the individual is who he says.
VU Mobile Token

It is a mobile application that generates one-time password (OTP) which can be used to ensure the identity of a user when using a computer system.

VU Mobile Multi Token

Meets VU Mobile Token functionality by adding the ability to integrate multiple tokens in the same application, offering to the user the convenience of having all your systems centralized identification. The application supports multiple VUID’s and multiple validation services (VPN, Web, eBanking, IVR).

VU Mobile Challenge Response

By implementing customer VU Mobile Challenge Response authentication system will implement a system that needed an OTP delivered by the server to calculate each OTP code.

VU SMS Token

Allows sending one-time password via SMS (Short Messaging Services) to 100% of mobile devices. The service can work in single track mode, the user only receives the password only once or twice in the mode via which the user receives a code and should send another SMS to complete the validation process. This module can also be integrated via USSD.

VU Sync Token

The evolution of online identity validation with this solution systems users will not have to worry about or remember complex codes enter contraseñas extensive. With VU Sync Token just enough to "authorize" each transaction and the mobile device is responsible for establishing a secure communication eg your bank and verify that the conditions exist for such transaction minimizing potential fraud or identity theft attack.
Implementation HOTP

VU Security solutions implemented HOTP algorithm specifications. HOTP generator algorithm is a one-time password-based HMAC specified by the IETF. As a general rule, VU Security work based on standards and specifications backed worldwide.

Technical Specification: RFC 4226

Implementation de TOTP:

TOTP (Time Based One Time Password) for its acronym in English Time Based One Time Password Algorithm is an extension of the already tested HMAC-Based One Time Password. TOPT implementation uses a scheme whereby lets give it a short lifetime each OTP.

Technical Specification: RFC 6238

Implementation VUOTP:

VUOTP (One Time Password Security VU): VU Security has a generation method, validation and authentication OTP’s owners, by allowing you to work simultaneously with a set of events, time and patterns authentication. This mode gives the customer the opportunity to choose a variety of options and generate your propie strong authentication scheme.

Implementation OATH:

OATH: Open System authentication, which allows providers robust authentication solutions coexist under one infraesctructura. VU Security solutions are compatible with this standard uqe allow integration with other brands and solutions on the market.

Technical Specification: Release 2.0
http://www.openauthentication.org/webfm_send/1
**Customizing algorithm**

VU Security is different from the market in general to have the capability to customize the algorithm for the exclusive use of the client, in this way
You can have a single SEED in the world that minimizes risks of exploitation of vulnerabilities.

**Differentials**

Multi Token: just a token for all remote applications.

Intuitive: the user only has to enter the Phone PIN and wait for the application automatically granted Ia One Time Password (OTP).

No limits: Works on any device that supports J2ME, iOS, Android, Blackberry and USSD.

Practical: The not rely on cellular networks, Internet or text messages, while avoiding doing al user delays in using their systems.

Economic: Al work 100% digitally Ia each Mobile Token replacement is simple, free, fast and user friendly for anyone who has forgotten, lost or broken your mobile device.
VU Security

VU Security is the leading developer of security solutions that prevent online fraud and identity theft company. We provide solutions focused on information security to individuals and businesses and government agencies. Our solutions protect against pharming attacks, phishing, man in the middle, vishing and botnets, among others. VU Security’s mission is to maintain the confidentiality, integrity and availability before, during and after a transaction validation credentials.

Capacity for innovation

Since its inception the company founders focused on developing technology solutions that fit the needs of users, simplifying and relaxing use for security purposes. Recently, Banks and Government agencies VU Security Argentina elected to have checked the level of innovation, commitment and response time. Recently, VU Security has launched a solution that can integrate to any system of double factor authentication through the implementation of VU in Application Server mode Cloud Services.

Deployment scenarios:

VU Security solutions can be integrated into any process of authentication or validation operations that use computer systems. Some of the most common and are used daily: Payment systems and financial access to corporate networks, accounting systems, Access VPNs, Intranets, Email, Home Banking, Web sites, security systems (turnstiles, access to vaults ) or ATMs, CRM's, and / or IVR. Manufacturers such as Cisco Systems, Juniper, Citrix, Fortinet and Microsoft among others recommend and certify solutions VU Security.