



DES & 3DES Vocalid[®] v2.0 Card

A High Level Authentication Solution

Today the User Authentication coupled to a static Password is not offering the expected level of security for any kind of transactions.

Elva, based on its Vocalid Technology, has developed several very attractive authentication solutions using the DES, 3DES or Elva patented algorithms. They are extensively used where a high security level of authentication is required, i.e. online transactions, e-banking,

The authentication is based on the emission of an encrypted acoustic signal. This crypto acoustic process consists of sending online a 128 bit encrypted signal within an acoustic vehicle. It transmits a dynamic One Time Password (OTP), instead of the current Login, Password or Card iNumber, to provide a high security level of authentication.

The Vocalid V2.0 card uses the DES, 3 DES and Elva property patented algorithms

The chip is a standard component dedicated to the Smart Card applications. Vocalid V2.0 card contains all the up to date inputs to keep confidential all the data.

The Acoustic Authentication

The Vocalid technology, patented by Elva, is bringing a brand new and user friendly solution to the user's authentication.

This new and very attractive solution is based on a secured Microcontroller dedicated to the smart Card applications. The Vocalid V2.0 card is ISO 7816 and SIM compliant.

When activated, the Vocalid V2.0 card transmits repeatedly through its acoustic interface a FSK modulation named Authentication Sequence.

This Sequence is a 128 bit One Time Password (OTP) associated to a unique Identification Number. At the end of the personalization process, the card memory is locked and cannot be modified anymore.

A new cryptogram is calculated by the card each time the acoustic interface is activated and then stored into the card memory.

A DES, 3 DES or property algorithm is used to generate the cryptogram.

The 128 bit acoustic encrypted signal is transmitted through the microphone of the fix telephone, cellular phone or PC to a dedicated server.

The server of the Vocalid system contains a database where individual accounts are created. Each Vocalid V2.0 card is associated with an account and all card related data are stored in the data base.

After the extraction of the Identification number of the card, this number is used as an index by the server to retrieve all the data associated with the card.

The check is based on the fact that the last cryptogram received by the server is correct.

Therefore, the proof is made that the card currently sending its authentication sequence is a genuine one and is the one associated with the account pointed by the Identification Number.

This process avoid any mistake or misuse from the user, knowing tat the acoustic sequence is unique.

How to use Vocalid v2.0

Vocalid V2.0 card is really user friendly.

Introduce the smart card Vocalid V2.0 into the External Acoustic Module (EAM).

Approach the module close by the microphone of the fix telephone, cellular phone or PC and gently press the botton for a couple of seconds, up to the point that the acoustic sequence is fully transmitted.

Vocalid V2.0 card. The evolution

The introduction of this new generation of Vocalid V2.0 card is bringing a hudge potential of applications.

Vocalid V2.0 card is a firmware solution brought on a standard smart card platform.

Therefore Vocalid V2.0 can be embedded into a standard smart card chip to be added to the current applications as for example banking card.

Upon request Vocalid V2.0 card is able to integrate new authentication algorithms.



EAM activator and Vocalid v2.0 card



SIM Card

Main Characteristics

SecureAVR™ smartcard microcontroller
FSK tone generator
Low voltage operation: 2.5V to 5.5V
ISO 7816-3 Compliant
High Security microcontroller
64 bit Identification number
Patented Authentication Protocol, DES and 3DES Algorithms
64 bit or 128 bit secrete seed
24 bit Secure Code
Secure Code Attempts Counter
High Reliability
Endurance : 500,000 cycles
Data Retention : 100 Years
ESD Protection : 4,000 V min



ELVA SA.
72-74 Avenue Edouard Vaillant
92100 BOULOGNE - France
Tel : + 33 (0)1 41 31 66 77
Fax : + 33 (0)1 41 31 66 70
<http://www.elva.fr>