

DIGIPASS® Controller

Worried about security leaks in your network? Or got convinced that static passwords are an invitation to hackers? No need to start ripping open your smoothly running application. The Digipass® Controller is the solution to end your nightmares immediately.

Just link the Digipass Controller to the application and let it handle all log-in requests. The only thing that has to be done in the meantime is to program a Digipass and get it to your users. And then just relax.

Easy to use

Digipass Controller has been designed by specialists in system entry security with just one idea in mind: make access control easy and yet safe for the non-specialists.

All that needs to be done is to add a field in the existing user database describing the new Digipass assigned to the user, and from there the DIGIPASS Controller will be able to check the dynamic password. And dynamic here really means what it stands for: from a one-time password to full signatures over a message, using either Response-Only or Challenge/Response authentication schemes.

Enabling applications

The DIGIPASS Controller is a real "enabler" of remotely accessible applications. And those applications cover a wide and in fact unlimited range going from simple remote access to data, over different kinds of electronic banking to full-fledged e-

commerce solutions. Today these applications often are closed for a wide range of users because of the existing risk inherent to open access. Now that same system and its applications can be opened to a wide range of users without giving in a bit on security. The combination of Digipass Controller and Digipass offers strong authentication and digital signatures in different flavours such as time and/or event based. Your users will be largely grateful because the remote access becomes fully automated without long telephone calls through secretaries to get the information they need urgently. Now they just get it straight from the server, which is also preventing human errors in the look-up and transfer of the information.

Zero knowledge integration

Integration of strong authentication was up till now often a choice between a specific access control server and a do-it-yourself job. The first solution offers easy-to-install

possibilities but is sometimes hard to configure. The second solution puts an unnecessary burden on your IT department without any guarantee that the final result will in fact offer the required security. VASCO has bundled its experience in both domains into this API type solution. Just add the few necessary calls in your application and you are up and running. And the future is bright because with a maintenance contract you are sure that your access control system will follow the latest trends in encryption technology and standards. Any subsequent upgrade will install with the same ease as upgrading a driver on a system.

Multi-platform

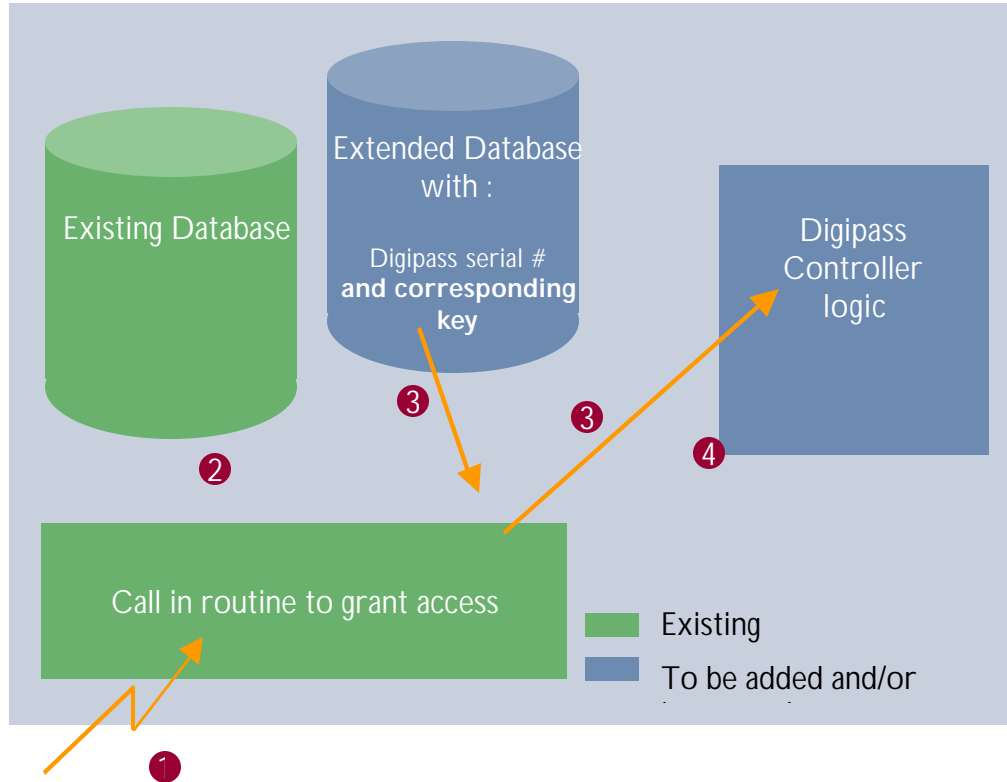
VASCO takes care of your investment by providing solutions for almost every operating system. These platforms range from Intel platforms to large mainframes each with its own requirements and means of input of the Digipass Controller software. And although the platforms differ, the means of access remains the renowned VASCO Digipass technology. And the system allows mixing any number of Digipass in the system at the same time.

A proven solution

Currently the Digipass Controller has proven its quality and stability in many different environments. More and more IT managers prefer their engineers to put their time in the company's target developments and source the unknown extra's from experts in their own field.

Key features:

- Fully application independent, easy to use API calls
- Support for Little-Endian and Big-Endian processors
- ASCII and EBCDIC support
- 16-bit to 64-bit memory support
- Multi-thread and multi-task aware code
- Compatible with the complete current and future line of VASCO's Digipass token family
- Support of different authentication modes:
 - Response only
 - Challenge/Response
 - Signature
- Support of DES and triple DES
- Integrated secure unlocking feature for locked users
- Helpdesk support
- Maintenance contracts available for upgrading
- Full set of working integration samples



- ① User calls in on the existing application providing his log-in name and the dynamic password generated by his Digipass.
- ② The existing application routine looks up the user in its database where the Digipass information was added.
- ③ The Digipass information is sent to the Digipass Controller.
- ④ The DIGIPASS Controller verifies the Digipass information and sends the GO/NO GO result to the access granting part of the existing application.

Feel free to contact us for more information

VASCO DATA SECURITY, Inc.
 1901 South Meyers Road, Suite 210
 Oakbrook Terrace, Illinois 60181, USA
 Tél. : +1.630.932.8844
 Fax : +1.630.932.8852
 E-mail : info_usa@vasco.com

VASCO DATA SECURITY nv/sa
 Koningin Astridlaan 164
 B-1780 Wemmel, Belgique
 Tél. : +32.2.456.98.10
 Fax : +32.2.456.98.20
 E-mail : info_europe@vasco.com

VASCO DATA SECURITY FRANCE S.A.
 481, boulevard Alfred Daney
 F-33300 Bordeaux, France
 Tél. : +33.557.19.11.00
 Fax : +33.557.19.11.09
 E-mail : info_france@vasco.com