

DetectID STRONG AUTHENTICATION SOLUTION

Highlights

- | *Pushes protection where it is most needed – the consumer device.*
- | *Strong authentication via hardware device authentication.*
- | *Effective protection against phishing and any kind of identity theft attacks.*
- | *Multifactor authentication that raises the security bar to avoid phishing attacks.*
- | *Easy to implement and deploy across unlimited number of users.*

DetectID is an innovative authentication solution to implement a two factor authentication scheme using a proprietary patent-pending algorithm by extending the authentication process to the device where the transactions are being launched.

Working at the device level, DetectID captures hardware specific information that is used to feed the proprietary algorithm to define a device fingerprint.

This scheme allows creating two factor strong authentication scenarios where the user/password combination is tied to devices based on which DetectID can define, in real time, the level of confidence that can be expected from any Internet banking session at any given moment.

DetectID is the first step toward reducing the risk of compromising end users with identity theft attacks, phishing attacks and ultimately the loss of Money and confidence in the Internet as the most effective and cost reducing transactional vehicle.

DetectID Features

Device Authentication

100% hardware authentication engine able to univocally authenticate devices running Windows, Linux or Mac

Security Image Authentication

Using this characteristic each user defines a secret image that allow the user to verify that they are indeed at the bank's website and not at some scammer's fake site.

Challenge Question Authentication

This additional authentication scheme is launched when a user is attempting to login into the system from a no-enrolled device. Maximizing this way user mobility and flexibility without losing security strength.

Additional Authentication Schemes

DetectID is loaded with out of the box additional authentication schemes like virtual/physical grid card authentication and could also be integrated with external OTP technologies via Detect Professional Services.

User's Device White Lists

This feature allows an end user to enroll more than one device as a valid token for the strong authentication system implemented using device authentication.

Institution's Device Black Lists

Once a device is detected trying to carry out fraudulent activity, its fingerprint is added to the institutional blacklist. In this way is possible to anticipate fraudulent activity. Furthermore, Easy Solutions via SSU (Special Security Updates) populates the black list database with malicious fingerprint found around the world. All customers benefits from the world-wide collective experience.

Easy Implementation

DetectID has been designed and developed for easy integration with the customer's current business and security environment. DetectID supports web services to reduce the amount of code that has to be added in the authentication routine of the current web application.

DetectID Benefits

Rapid Implementation

With DetectID one implementation enables security for the whole on-line community eliminating additional activation.

Extended Platform and Browser Support

DetectID is a proven technology over Windows, Linux, Mac with browsers like: Internet Explorer, Firefox and Safari.

Cost Saving

Online fraud related to phishing and malware amounts to millions of dollars of losses per year. In most cases, financial institutions have assumed the liability for these losses. DetectID tackles phishing and the emerging designer malware threats to significantly limit financial losses.

*Start protecting your
online transactions with*

DetectID!
sales@easysol.net