

Online Identity Assurance closes door to unwanted and fake visitor

Date: 01-08-2009 06:36 PM CET

Category: [IT, New Media & Software](#)

Press release from: [ID Control BV](#)



The Hague, 9 January 2009, ID Control, the specialist in advanced online identity and access management today announced to fight online identity theft and fraud with a hassle free managed service by which users' identities are protected with strong and advanced authentication tokens based on a monthly fee per user.

Starting at 2.50 Euros per month per user the right users are protected by strong and advanced authentication solutions. The identity of the user can be verified with one-time-password authentication based on mobile phones or OTP hardware token or verification of the user's typing behaviour during login, before granting access after checking the permission rights.

Most organizations that operate online, offer their clients, partners, suppliers or employees access to private or sensitive online services and information or let them perform transactions. Controlling the identity and access of the users to systems, networks and applications are ranked high in priority on the list of security measures nowadays. Strong authentication is based on the principle of "something you know (password/PIN)" and "something you have (authentication token)", or "something you are (biometrics)" and is therefore more secure than only username and password. With a secure and affordable identity assurance service the organization decides on the strong authentication needs, demands and wishes to be managed while paying only on a monthly basis for the usage of the service. With the online Identity Assurance of ID Control no implementation and maintenance of an authentication infrastructure is required, by making use of the already existing and pluggable infrastructure and expertise of ID Control's broad partner network. All hardware, security, infrastructure and software components and services needed for implementing and maintaining the authentication management environment are taken care of. This means ID Control Server software, web based management interface, ID Control authentication tokens like HandyID, MessageID, KeystrokeID and ID Control OTP Key and the maintenance and support by an external highly qualified engineer are included or optional.

Hans Kortekaas, CEO ID Control, indicates that ID Control provides this managed strong authentication service with standard integration to existing web mail, server based computing, SSL VPN, web applications and network environments, while taking away the hassle and burden of its management. The customer does not need to invest in hardware, authentication tokens,

software, implementation, trainings, helpdesk, maintenance and support and can adapt to authentication needs in the future. With ID Control's online Identity Assurance you are secured by the best and most advanced identity and access management solutions and services in the industry while diminishing the risks and threats related to online identity theft and fraud.

ID Control, www.idcontrol.com located in The Hague, provides next to One Time Password generating hardware tokens with OTP the "ID Control OTP Key", OTP based on mobile phones with "MessageID" a generated OTP by SMS, "HandyID" a mobile OTP application and PKI the "ID Control USB Token", but can also recognize users on the basis of their typing behaviour with "KeystrokeID" while logging in. All tokens are managed by ID Control Server hosted at the partner's or customer's side, by which user are strongly authenticated. Above all organizations with different authentication methods and tokens for a variety of systems, applications, users and services can manage all of them in one web based central authentication environment with the "ID Control Server".

Should you have any questions, and/or remarks, please do not hesitate to contact Susan de Wolf at +31 (0) 888-SECURE (732873).

Susan de Wolf
ID Control BV
www.idcontrol.com

[You can find this press release here](#)