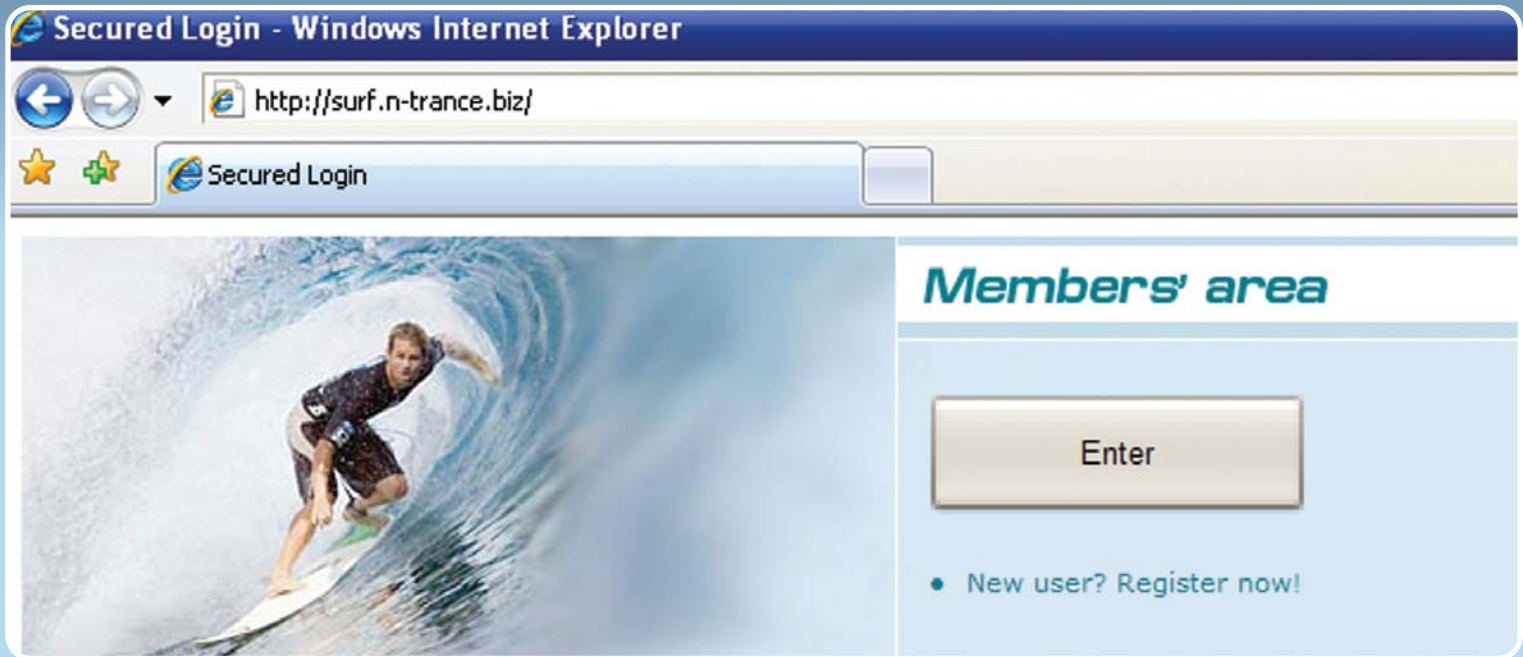


n-Surf : The Secured WEB login

where security meets convenience...



What is authentication?

Authentication of a person is the act of establishing or confirming someone as authentic. Usually authentication is necessary to access a system, an application or a website. In these cases, it confirms that claims made about the person are true.

In IT, "authentication" is a way to ensure that users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.

How is authentication done today.

Most websites use a standard authentication method, when a user claims their identity with a username and confirms with a password.

This method has three major drawbacks...

First, everyone who knows the username and password is identified as a valid user. Another drawback lies in the complexity of storage and operation of the database of users. This database shall be stored securely, it attracts hackers' attacks, and its protection demands additional efforts.

The last, but not the least problem is the human factor. User cannot remember complicated password and, therefore, the calls for support are 80% requests to reset or remind password; alternatively user usually selects simple password, which in turn compromises security.

The authentication requires one factor identification with two parameters:

Something you know – Like a User name or Email address.

Something you know – like a password or a PIN code

Unfortunately, these two parameters are not sufficient. While you want to grant the user an access to a highly secured WEB site (financial transaction etc.), it has been proved that the Password or PIN code are factors that can be easily traced, tracked, and cracked. This fact requires another challenge that would allow for higher secured factor identification, yet, with an easy and friendly user interface.

How can we increase the authentication security, and still keep the process friendly?

The solution is to add second or third security layers with additional identification factors: Something you have, and something you are.

In our case:

Something you have – a USB biometric Pen Drive, the n-Tegrity

Something you are – the user's fingerprint.

Although, we have increased the security layers with two identification factors, the user's interface has become easier to use. In addition, implementing the n-Surf authentication application makes the authentication mechanism extra safe from identity theft.

n-Surf : The Secured WEB login

where security meets convenience...

What is n-Surf?

n-Surf is the ultimate easy and secured way to perform authentication of registered users within less than a second, using strong patent pending PKI-based technology.

Nothing to fill-in, nothing to type and nothing to remember

A very important and critical factor – the procedure does not demand ANY installation on the client side. Just plug the n-Tegrity biometric key, unlock it with a fingertip and click “login”

How does it work?

Registration:

During the registration process (first time), user's public key and other information are filled-in automatically by n-Pass Pro (Part of the n-Tegrity biometric key) and stored in database on the server. No secret/personal/unwanted information, neither fingerprint template(s) is sent to or stored on the server! Even password or its hash is not required for the secured authentication

The Authentication process:

When a registered user approaches the secured webpage, the server generates a random string with a time-stamp (for example – 5 minutes to authenticate), which looks like following:

```
30444798b1cc1d77ccGGMflAbkgPnK76VV3VdFtzhzeX9TuoghB2mOikOilMBrlt9ouOH9N9aOxNgtS2tL1
MvK3DEuyP8c6nGHR1OuRODcwq36I92UTVQPgz6UxX2QP7eQuRclw6R1OkganuXswlObXi6qzfl9z23Tz
KnPcrft1ddmWxPIN6dkISyhAscIdDNNovX5c24F6a296ZLmk5jBBZvky7L4jwTiksockYVLuew16eeJLBlcn9
whMZWjAMczPvlfStRNZ3hnB.
```

The n-Pass captures this string, digitally signs it using private key from RSA-2048 key pair and returns to the server together with any publicly available users information e.g. e-mail address or username (This information is required to retrieve user's public key from the database). The signed key looks like:

```
22d932788eee032e7be971fbfbfdd8be317e4198f5509190625320708c6467a577f8f12b0f2c5102ad073e37
4e66ac53c9adc37879dde50a9eceb17cccd23c5c4508d6321fdcea33b439457cb0acc40d7453c9e83b9d0a
ac002a84921c303966ac08edfe4e609878f7744c074637aa86bc3b5764112b7a588faebb3c8ad8499a2f3ad
7b035516a8cbe3448e9e23ac8fb1c652835112b80ad9187ca62112c0183f8dbd94511144fb1ba281da821c1
488df0b5e7ff0c8203e15363b48bd2b4a9a0cb2ab0eff1e30ec432e056af52a475c8031613b58d6234634231
18b6f8da407d52308f522745d83fe584db4a14e3bcaba8d1ad077628e0eac9dd32317d6d2fa0
```

The server verifies the signature. After a positive verification, the user is logged in. The process does not require more than 1 second.

Advantages

The n-Surf authentication is much easier and user friendly than any old scenario utilizing username/passwords. Not only for users, but server administrators can benefit from using the n-Surf.

Administrators are not obliged to store passwords, nor required to reset them, and there is no threat of identity theft anymore. The WEB login is secured in a way that it is clear that the authorized persons are really the ones that attempt to log in.

The advantage of this identification factor are enormous to many secured WEB sites, secured applications, and their users. more. The WEB login is secured in a way that it is clear that the authorized persons are really the ones that attempts to log in. The advantage of this identification factor are enormous to many secured WEB sites, secured applications, and their users.

