

all-factor authentication

Volume 1
Issue 1
Sept 2010

SafeTok News



“It’s Networkers not Networks”

It’s staggering to find that approximately 40% of all help desk calls are related to password issues. According to Gartner each password related call to a help desk costs around US\$22 or US\$150 per user per year.”



“In a recession, levels of crime, in particular theft of company and supply chain data, rise considerably. Over the next year we are going to see more highly targeted attacks.”



What is all-factor authentication?

“All factor authentication is a fast emerging identity and access management technology which is becoming increasingly relevant as organisations deploy a wider range of risk related user authentication processes in order to comply with a fast changing threat landscape.”

All-factor Authentication

Network security originated in the cold war era of the 1960s. This tightly integrated, military style command and control environment meant that only a limited number of factors were needed to identify authorized users. This legacy created the “User name and Password” security structure we still have with us 50 years later. However we now live in a world where everyone, everything, everywhere is connected.

The majority of this connectedness is via the public Internet where it is less easy to authenticate a user’s true identity. This created an opportunity for cyber criminals changing the security threat landscape from cold war to cold cash. The appearance of multiple threats together with more intrusive regulation, created the need for multi factor authentication. However multi factor authentication doesn’t protect against all risks.

To secure a network against all risks you need all-factor authentication.

All factor authentication is a fast emerging identity and access management technology which is becoming increasingly relevant as organisations deploy a wider range of risk related user authentication processes in order to comply with a fast changing threat landscape.

SafeTok is a cost effective solution for organisations wishing to deploy all-factor authentication.

IN THIS ISSUE:

- What is all-factor authentication?
- Taking all factors into account.
- Safetok authentication process



Your key to the secure web

www.safetok.com
Styskin's Solutions Limited

Taking all factors into account.

- What you know - password
- What you have - device
- Who you are – fingerprint

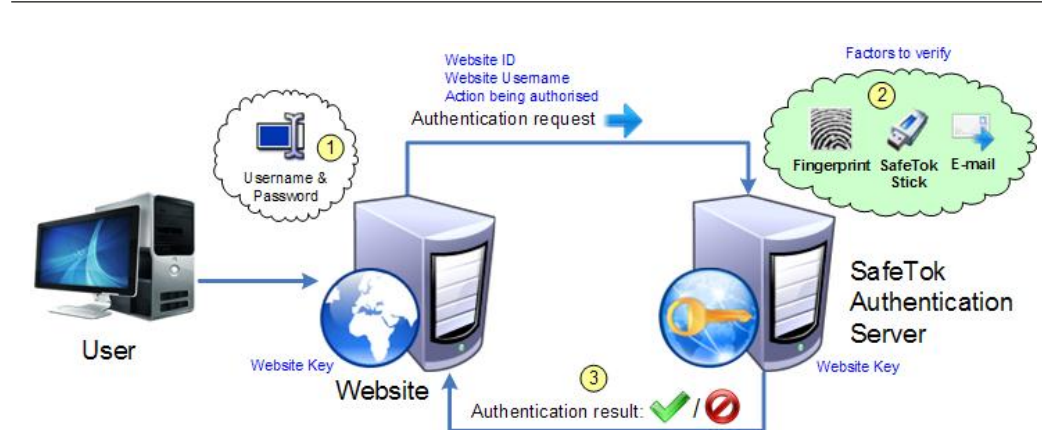
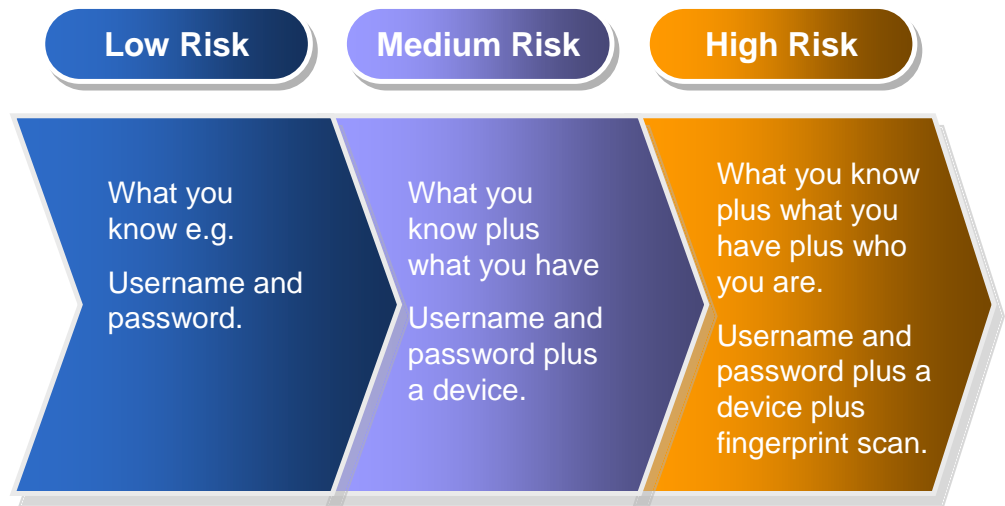
Encrypted Devices include:

- USB sticks
- Memory cards
- Hard Disc Drives
- Network Drives
- External HDD
- Solid State Drives



Protection includes:

- Automatic Phishing detection
- Man-In-The-Middle prevention
- Man-In-The-Browser prevention
- Unique feature device lock-in
- Localized fingerprint verification
- Obfuscated fingerprint storage
- Multi-channel SSL communication
- Multi-hop SSL validation
- Local transaction transcription



The SafeTok authentication process.

Step 1. The user provides a username & password.

Step 2. If the username and password are verified, the user is redirected to the SafeTok Authentication Server, where all additional protection factors are processed. If required, the user can be prompted to confirm an action such as an online purchase or money transfer.

Step 3. The SafeTok Authentication Server redirects the user back to the Website and informs the Website whether the user has passed the authentication process successfully or if there were any problems.

The advantages of "Authentication as a Service"

One of the important differences of SafeTok is the concept of "authentication as a service". This design offers a number of advantages, both in terms of convenience and enhanced security:

- two separate independent authentication servers - two layers of security
- no long term commitment – join and leave as required
- no extra software to install on your existing website server

Styskin's Solutions Limited
01257 401 942 Mobile 07500 848 672
Germany: + 49 171 8014 249
Netherlands: +31 648 313 398
ken.garner@safetok.com
www.safetok.com