

---

# SAFETOK ADAPTIVE AUTHENTICATION SYSTEM

---

## *A SafeTok White Paper*

Ken Garner  
Business Development Manager  
Styskin's Solutions Limited

# Contents

<b>Purpose and Scope .....</b>	<b>1</b>
<b>Introduction.....</b>	<b>1</b>
<b>How Does SafeTok Work?.....</b>	<b>3</b>
What Protection Does SafeTok Provide? .....	4
UK And International Compliance.....	4
SafeTok and European Jurisdictions.....	5
The Economics of Compliance.....	6
SafeTok Authentication Process Schematic overview.....	7
Conclusion.....	8

## List of Figures

Figure B.7-1. <i>Main Network Access &amp; Authentication Issues</i> .....	2
Figure B.7-2. <i>Compliance Issues and Safetok</i> .....	4

## Purpose and Scope

This SafeTok white paper is designed to provide an overview of the UK and international regulatory and data security threat landscape together with an understanding of the workflow problems and logistical issues surrounding current network authentication and access technology. The paper will focus in particular on the problems associated with single factor authentication and password recycling. This paper explains the SafeTok Adaptive Authentication System and is aimed at personnel who are responsible for assessing PCI DSS and Data Protection Act compliance, implementing, performing or reviewing network access, information security processes, managing data loss policies, developing supply chain compliance strategies and supervising data users.

## Introduction

Access to up-to-date information delivers competitive advantage. Technology makes information readily accessible and available to share, within the enterprise, with clients and suppliers and throughout the extended supply chain.

Sharing information increases productivity, but sharing sensitive company or personal data raises issues about data loss or the misuse of confidential data by third parties.

The data threat landscape is changing very rapidly. The UK Information Commissioners Office (ICO) has recently gained new powers of entry and inspection without notification.<sup>1</sup> Provisions introduced in 2010 contained in the 2008 Criminal Justice and Immigration Act will enable the ICO to impose fines of up to £500,000 on organisations where there is evidence of reckless or deliberate data protection breaches.<sup>2</sup>

The ICO is also re-defining their existing powers under the Data Protection Act (DPA) 1998.<sup>3</sup> Policies are no longer enough, they have to be visibly and transparently enforced. Recent ICO adjudications have reinforced the principle that the provisions of the DPA 1998 take precedence over any existing policies, standards, accreditations or prior working practices.<sup>4</sup>

At the same time cybercriminals are mounting increasingly sophisticated, highly targeted attacks using techniques derived from internet grooming, targeting employees of companies with access to valuable or sensitive data.

Recession induced lay offs also creates data risks. It's not just those who leave taking data with them. Remaining, often overstretched staff, begin making mistakes, sharing or reusing login credentials and putting company data and reputations on the line.

Because we live in a world where everyone, everything, everywhere is connected, data has to flow to wherever it is needed; an organisations actual perimeter is no longer its physical or legal boundary.

---

<sup>1</sup> The press release announcing these new powers can be viewed at [http://www.ico.gov.uk/upload/documents/pressreleases/2008/statement\\_new\\_powers.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2008/statement_new_powers.pdf)

<sup>2</sup> The CJA 2008 can be viewed at <http://www.justice.gov.uk/news/newsrelease090508b.htm>

<sup>3</sup> A summary of the DPA 1998 can be viewed at [http://www.ico.gov.uk/what\\_we\\_cover/data\\_protection.aspx](http://www.ico.gov.uk/what_we_cover/data_protection.aspx)

<sup>4</sup> A summary of recent adjudications is at [http://www.ico.gov.uk/what\\_we\\_cover/data\\_protection/enforcement.aspx](http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx)

The security focus is moving from hardware on the network edge and onto the data user with the spotlight firmly on Adaptive authentication as the only workable solution. Adaptive authentication addresses three main business issues. It reduces the risk of data loss. It helps companies comply with legal and professional regulatory requirements and builds supply chain trust by demonstrating commitment to data security.

Most companies will have network access and security policies already in place ranging from Acceptable Use Policies, Information Protection Policies, HR Policies and Employment Contracts. Many will also have contractually imposed Information and IP protection safeguards imposed by upstream suppliers and downstream customers.

However a significant number of information security breaches come about as a result of employees' failure to comply with existing, well documented, security practices and policies. Many organisations have tried to sustainably modify user behavior towards password security. Almost all have found it difficult, if not impossible. Research has shown that most of these data security breaches are caused by security mechanisms which are either technically complex or have become an impediment to the user completing their work in a timely fashion.<sup>5</sup> It's called workflow friction.

Even technically competent users such as systems administrators and software developers often struggle to keep up with the ever increasing complexity and administrative workload created by GRC, DLP and network security processes.<sup>6</sup>

The goal has to be to provide "practical network security" using versatile tools which non technical end users can operate correctly with little or no training, which have minimal impact on existing network infrastructure and working practices and which work within irregular, dynamic, often unstructured environments where the user might have multiple passwords, to multiple systems from multiple end points.<sup>7</sup>

Issue	Effect
"Static" Single Factor Authentication	Inherently insecure, poor security practice
"Dynamic" Single Factor Authentication	User workflow is interrupted and productivity is decreased, many users find a workaround.
User generated of passwords	High risk of insecure passwords or passwords being transmitted "in the clear" compromising data security
Early Multifactor Authentication	Data can still get into the wrong hands
No audit or tracking	Who is or isn't using secure passwords?
No password expiry	The data is at risk ad infinitum
No Authentication time out.	Attacker can still gain access

**Figure B.7-1. Main Network Access & Authentication Issues**

<sup>5</sup> Whitten, A. & Tygar, J. D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999, Washington 1999.

<sup>6</sup> Yee, K P. (2005) User Interaction Design for Secure Systems. In L. Faith Cranor & S. Garfinkel [Eds.]: Security and Usability: Designing secure systems that people can use 2005. pp 13-30. O'Reilly Books.

<sup>7</sup> Zurko, M. E. & Simon, R. T. User-Centered Security. New Security Paradigms Workshop 1997.

SafeTok from Styskin's Solutions Limited is a unique solution to the problem of employee resistance to using secure access. It's modular, integrated, easy to learn and use, little or no training is required, no changes are needed to current IT systems or infrastructure and there are no changes to established working practices or workflow. SafeTok achieves this by balancing usability, security, productivity and compliance.

## How Does SafeTok Work?

The basis of the SafeTok system is the concept of "Adaptive authentication". Adaptive authentication provides the ability to connect securely to multiple applications, each with their own login and password, where those passwords can be retired and changed as frequently as is necessary, where those changes can be "pushed" to the SafeTok device and where either single, 2 factor or 3 factor authentication can be imposed dynamically based on the current perceived threat or risk.

The SafeTok authentication server manages this process and provides a secure encrypted communication system, logs authentication events and generates comprehensive management compliance reports.

Authentication stages two and three work as follows:

**Device authentication (2nd factor)**. In the SafeTok system, users can choose one or more devices to provide secure access to his or her account.

Without these security devices no other person can log-in to the user's account. They act just like keys, all the user has to do to enter the account is to connect one of the SafeTok enabled devices to the computer.

SafeTok devices can protect multiple accounts on multiple websites. The whole authentication process is completely automated - there is no need for the user to type any sort of authentication codes. In the background, innovative SafeTok authentication technologies (such as automatic Phishing and Man-In-The-Middle detection) protect users from all known cyber-attacks. Users do not need to worry about clicking on links in e-mails or try to verify SSL certificates.

**Fingerprint verification (3rd factor)**. SafeTok allows users to protect their accounts using fingerprints. These are the most secure and reliable type of personal biometrics available. To login, just scan a finger over the SafeTok USB drive fingerprint sensor. Once verified only the true owner will get access.

- A SafeTok USB drive can store non sensitive files without fingerprint protection.
- Confidential files are stored in the USB drive using fingerprint protection
- One device secures multiple accounts
- Password resets can be "pushed" to the SafeTok device
- More complex and therefore more secure passwords can be used.
- The password is not revealed to any unauthorized person at any time.<sup>8</sup>

---

<sup>8</sup> Password Research Institute. Improving password security and authentication.  
<http://www.passwordresearch.com/papers/pubindex.html>.

The categories that benefit from SafeTok protection most are:

- online banking
- online payment systems
- social networks
- corporate access to company website
- webmail
- online auctions, online shops, etc.

## What Protection Does SafeTok Provide?

- Your accounts are safe against all types of cyber attacks
- You are protected with the highest possible level of security.
- With SafeTok Biometric, even if you lose your SafeTok device your accounts are still safe, thanks to the fingerprint verification.
- Your fingerprints are stored encrypted solely on your SafeTok device, they are never sent to anyone, ensuring complete privacy and security.
- Confirm important actions (e.g. money transfer) by swiping your finger - you have complete control over what you authorize.

## UK And International Compliance.

SafeTok can help to maintain compliance with a number of UK and international legislative requirements, information security standards, industry regulatory bodies and supply chain demands. The table in Figure B.7-2 shows just a sample of the many areas SafeTok assists with Governance, Regulation and Compliance (GRC).

Compliance Issue	SafeTok
UK Data Protection Act 1998	Meets the Information Commissioners requirement for verifiable secure network access.
European Data Protection Regulations	Provides compliance with Article 17 of Directive 95/46
Individual US state data protection laws	Meets all current individual US state laws
PCI DSS	Conforms to the Payment Card Industry Data Security Standard (PCI DSS) for the protection of stored cardholder data.
Sarbanes-Oxley (SOX)	Provides secure access, data protection, audit and management reports as required under SOX
HIPAA	Delivers full conformity with HIPAA mandatory secure access to medical record files plus verifiable audit trail and reports.
ISO 27001/ISO 17799	Ensures ongoing compliance with sections 10.8.0 to 10.8.5
CobIT and ITIL	Compliance via link with ISO 27001/ISO 17799
Lexcel (UK)	Helps conformity with Lexcel 4A.2
Code of Connection (CoCo)	Helps maintain compliance with Sections 2.10 and 2.23
Other International Jurisdictions	SafeTok provides authentication compliance in most other international jurisdictions, see note below and page 5

**Figure B.7-2. Compliance Issues and SafeTok**

For more information about other international data protection jurisdictions visit:  
[http://www.accurateinformationsystems.com/docs/International\\_Data\\_Protection\\_Laws.pdf](http://www.accurateinformationsystems.com/docs/International_Data_Protection_Laws.pdf)  
 See also [http://datalossdb.org/us\\_states](http://datalossdb.org/us_states) and [http://datalossdb.org/us\\_federal\\_bills](http://datalossdb.org/us_federal_bills)

## SafeTok and European Jurisdictions.

Across Europe there are over 100 country specific public bodies devoted to ensuring that sensitive personal information held within computer systems or on computer devices, or transmitted across networks, is not accessed by or distributed to unauthorized individuals or agencies. All are tasked with ensuring that national laws transposing the European Directive on Protection of Personal Data are upheld; imposing obligations on public institutions, businesses and other organizations to protect personal data by deploying secure authentication and access systems. Implementation of the various European directives varies from jurisdiction to jurisdiction but secure login is the common denominator. As an Adaptive authentication solution, SafeTok meets the personal data protection standards of all the following regulatory bodies.

<b>Country</b>	<b>Agency</b>	<b>Website</b>
Austria	Data Protection Commissioner	<a href="http://www.dsk.gv.at/">http://www.dsk.gv.at/</a>
Belgium	Privacy Protection Commission	<a href="http://www.privacy.fgov.be">http://www.privacy.fgov.be</a>
Bulgaria	Personal Data Protection Commission	<a href="http://www.daits.government.bg">http://www.daits.government.bg</a>
Cyprus	Data Protection Commissioner	<a href="http://www.dataprotection.gov.cy">http://www.dataprotection.gov.cy</a>
Czech	Personal Data Protection Office	<a href="http://www.uoou.cz">http://www.uoou.cz</a>
Denmark	Data Protection Agency	<a href="http://www.datatilsynet.dk/">http://www.datatilsynet.dk/</a>
Estonia	Data Protection Inspectorate	<a href="http://www.dp.gov.ee/">http://www.dp.gov.ee/</a>
Finland	Data Protection Ombudsman	<a href="http://www.tietosuojafi/">http://www.tietosuojafi/</a>
France	Data Protection Authority	<a href="http://www.cnil.fr">http://www.cnil.fr</a>
Germany	Data Protection Commissioner	<a href="http://www.bfdi.bund.de/">http://www.bfdi.bund.de/</a>
Greece	Data Protection Authority	<a href="http://www.dpa.gr">http://www.dpa.gr</a>
Hungary	Data Protection Commissioner	<a href="http://abiweb.obh.hu/abi/">http://abiweb.obh.hu/abi/</a>
Iceland	Data Protection Authority	<a href="http://www.personuvernd.is">http://www.personuvernd.is</a>
Ireland	Data Protection Commissioner	<a href="http://www.dataprotection.ie">http://www.dataprotection.ie</a>
Italy	Data Protection Authority	<a href="http://www.garanteprivacy.it">http://www.garanteprivacy.it</a>
Latvia	Data Inspectorate	<a href="http://www.dvi.gov.lv/eng/">http://www.dvi.gov.lv/eng/</a>
Liechtenstein	Data Protection Unit	<a href="http://www.llv.li/amtstellen/llv-sds/">http://www.llv.li/amtstellen/llv-sds/</a>
Lithuania	Data Protection Inspectorate	<a href="http://www.ada.lt">http://www.ada.lt</a>
Luxembourg	Data Protection Commissioner	<a href="http://www.cnpd.lu">http://www.cnpd.lu</a>
Malta	Data Protection Commissioner	<a href="http://www.dataprotection.gov.mt/">http://www.dataprotection.gov.mt/</a>
Netherlands	Data Protection Authority	<a href="http://www.dutchdpa.nl/">http://www.dutchdpa.nl/</a>
Norway	Data Inspectorate	<a href="http://www.datatilsynet.no">http://www.datatilsynet.no</a>
Poland	Personal Data Bureau	<a href="http://www.giodo.gov.pl/">http://www.giodo.gov.pl/</a>
Portugal	Data Protection Commission	<a href="http://www.cnpd.pt/">http://www.cnpd.pt/</a>
Romania	Data Processing Supervisor	<a href="http://www.dataprotection.ro/">http://www.dataprotection.ro/</a>
Slovakia	Data Protection Office	<a href="http://www.dataprotection.gov.sk/">http://www.dataprotection.gov.sk/</a>
Slovenia	Information Commissioner	<a href="http://www.ip-rs.si/">http://www.ip-rs.si/</a>
Spain	Security Secretariat	<a href="http://www.mir.es/SES">http://www.mir.es/SES</a>
Sweden	Data Inspection Board	<a href="http://www.datainspektionen.se/">http://www.datainspektionen.se/</a>
UK	Information Commissioner	<a href="http://www.ico.gov.uk">http://www.ico.gov.uk</a>

## **The Economics of Compliance**

SafeTok has been designed and engineered from the ground up from the individual end users point of view. It's mainly individuals who cause data loss, it's individual end user behavior which has to be sustainably modified and it's individuals who choose whether to comply or not with the security policies governing their immediate work context.

Individuals choose whether or not to comply with security guidelines based on risk and reward or cost and benefit. There is a natural limit to the amount of effort users will expend on compliance unless there is a corresponding benefit.

Modern network security and digital encryption came out of the US military in the 1970s and 1980s.

The inflexible command and control structure of its original development environment created the network security structures and landscape we see today.

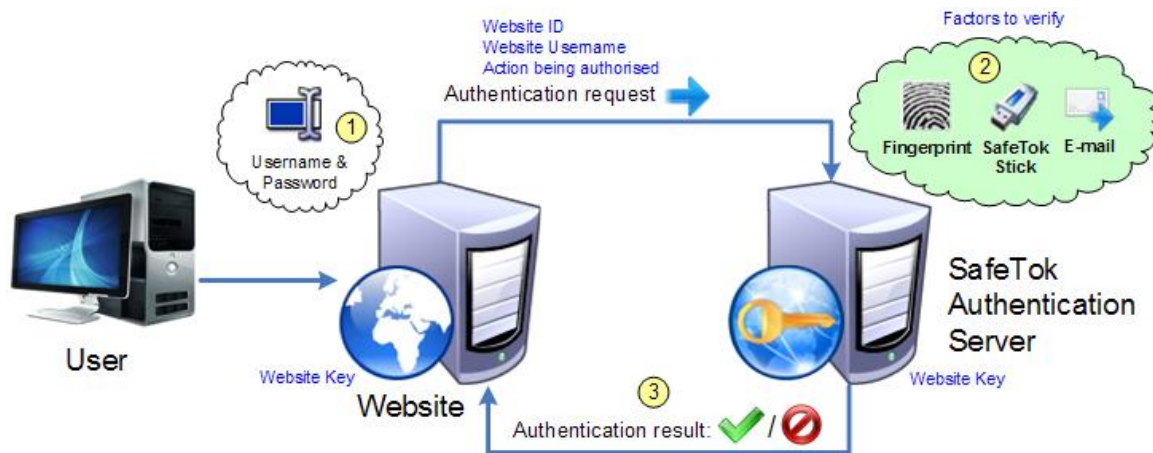
Within a fully integrated public or private organisation, with a standardized IT structure, secure login coupled with encryption offers nearly unbreakable information security. It's possible to demonstrate mathematically that it is computationally impossible to retrieve encrypted data without the encryption keys.

However even within a tightly integrated IT environment everyday practical issues in the deployment, maintenance and use of security technology have limited the business benefits and impaired the efficiency of business operations. Misapplied security increases risk, decreases protection, incurs unnecessary costs and reduces efficiency.

Until recently it has been almost impossible for organisations in extended supply chains, with dissimilar IT systems and differing attitudes to data protection to securely exchange confidential or personal data via the public internet without running substantial risks.

This is especially the case where data is only likely to be exchanged very infrequently or even on a one-off basis. The investment in infrastructure, training and skills outweighed the benefit of deploying compatible data security technologies.

## SafeTok Authentication Process Schematic overview.



### Authentication steps

1. User provides username & password, like before, to the website
2. If password is verified, the user is redirected to the SafeTok Authentication Server, where all additional protection factors are verified. If required, user can also be prompted to confirm an action, like a money transfer.
3. SafeTok Authentication Server redirects the user back to the Website and informs the Website whether the user has passed authentication successfully or if there were any problems.

### Advantages of "Authentication as a Service"

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

- two separate independent authentication servers
- two layers of security
- no obligation - should you choose to abandon SafeTok protection, it can be done at any time with no effort
- no extra software to install on your existing website server

## **Conclusion.**

In an increasingly tough business climate organisations have to decide how to spend their resources in the most effective way to achieve their operational goals.

It's important to protect client information, but the resources an organisation can deploy on information security are limited.

These limited resources have to be targeted to protect the most serious risk which is unauthorized network access and the theft or exposure of sensitive personal information.

Traditional network security is unwieldy for most users and the compliance cost is often greater than the benefit.

SafeTok is an Adaptive authentication solution which automates and deskills the entire network access process within a cost effective, secure, workflow based environment.

For more information contact SafeTok at [www.safetok.com](http://www.safetok.com)