# STRONG AUTHENTICATION TO A NETWORK OR WEBSITE

**Identity Verification is essential to the future of the online marketplace.**

The exponential growth of the Digital Economy has created many challenges for business-es in validating and protecting their users' private information.These and other impediments such as establishing trust in the online marketplace and verifying users are costing business multiple billions annually and impacting consumer confidence.

The threat of personal information: name, address, password, credit card details, etc. being regularly stolen for fraudulent use and monetary theft is constant and causing significant issues for all stakeholders of the digital economy. Consumer's credit cards can be used without their permission leading to their identity being exploited to create new accounts with online merchants for criminal activity.

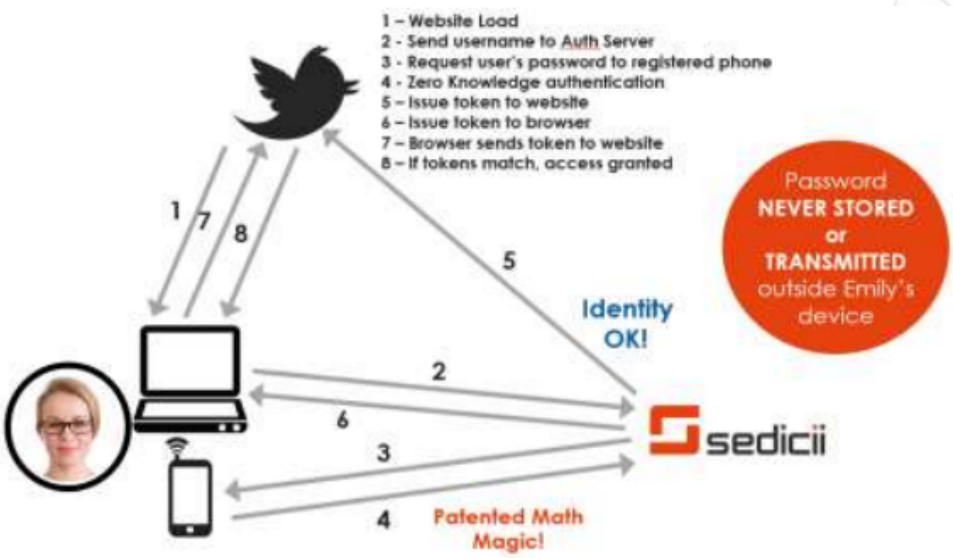
Verizon Enterprise reported 53k+ security incidents, in its 2018 Data Breach investigations Report. Non-compliance with EU GDPR carries penalties of up to €20m or 4% of global revenue and this takes no account of the costs to business of the breach itself. Sedicii's unique ZKP technology helps organisations to comply with strict AML and Data Protection legislation as no data is exposed during the authentication process.

## The Problem:

Usernames and passwords are a major problem for consumers of online services. They are too numerous to remember and don't provide effective security against account compromise where credentials are stolen through email phishing, malware on the computer or key loggers. A typical attack vector for an online banking solution may involve a customer receiving an email purporting to be from the customer's bank. Contained in the email is a link that the customer is invited to click. Once clicked the user is directed to a page that will appear to be their bank's website. However, it is a fake replica. The user, in many cases, will unwittingly be invited to enter their username and password for the site. Once entered it will be recorded for later re-use by the criminal. To counter this threat many online services are now requiring a two factor approach to account authentication, something you know (password) and something you have (a physical token) that will be required when the customer authenticates. The problem with many of these is that they are highly inconvenient for the customer as it requires them to carry a second device, such as a grid card, an OTP generator or a physical token.

## The Solution:

Sedicii has developed a two factor, strong authentication solution that increases security but not at the expense of convenience. In addition to the user having a password, the user's mobile phone is used as the second factor. The ID's embedded in the phone, IMEI (handset ID) and the IMSI (Subscriber ID or SIM) are combined with the unique password that only the customer knows to generate a unique signature for the user/handset combination. Using the power of the Sedicii authentication process, the user can be authenticated without this signature being exposed or exchanged.




*Sedicii Strong Authentication for Browsers*

## See Sedicii in Action...

A Sedicii demonstration can be arranged to experience the benefits of Sedicii Zero Knowledge Proof Verification in action.

To find about more or to set up a live demonstration, call or contact us using the details below.


**Sedicii Headquarters**
ArcLabs Research & Innovation Centre,
W.I.T. West Campus,
Carriganore, Waterford
Ireland. X91 P20H
Phone: +353 (0)51 302191

**Sedicii UK**
1-15 Clere St.
London
EC2A 4UY
Phone: +44 20 8144 8279

**Sedicii USA**
2F Plug and Play Techcenter
440 N. Wolfe Rd.
Sunnyvale CA94086
Phone: +1 408 786 5485

**Sedicii Tenerife**
C/Fotografo Jose Norberto
Rodriquez Diaz Zenon, 2
Piso 3 Oficina 3-5
Tenerife 38204

**Contact us online at:**
Web: www.sedicii.com
Email: contactus@sedicii.com
Twitter: @GRRSedicii


The process of logging into a website has changed from entering all credentials into a webpage via a single device to a split login process where you identify yourself on the website and complete the process on your mobile phone. The process used by Sedicii of splitting the login actions, is completed using zero knowledge proof patented technology. The advanced cryptographic algorithims used in the process provides huge improvements to security and privacy which is achieved with user consents and without impacting convenience for the user.

## The Value:

The majority of users want and demand convenience. They will accept a certain level of inconvenience in the interest of increased security. However, if that inconvenience crosses a threshold, the user will seek workarounds which will defeat the purpose or will have negative impact on customer satisfaction. Using the Sedicii Mobile Authenticator will:

- Increase security exponentially by eliminating email phishing as an attack vector due to the split login approach (for users that have smartphones)
- Increase security by eliminating the storage and transmission of the customer password while in either a fixed wire or wifi environment. Only the user knows their password and never shares it.
- Significantly reduce the likelihood of account takeover through the split two factor authentication approach, while maintaining convenience levels.
- Allow the user a strong authentication approach, by default, that can be reused with other services, thereby reducing the number of passwords they have to remember. Hence, increasing the security of all those services.
- Provides a method for non-repudiation of transactions as only the customer knows their private password and the smartphone must by theirs.
- Will contribute to an exponential reduction in fraud and the financial losses accruing from that fraud.
- As the organisation owning the service no longer stores the customer's password in a central repository, there is less attraction for a hacker to attempt to steal data.

## Commercial Considerations:

Sedicii can be deployed in an 'on premise' configuration where the client enterprise will manage and maintain the service entirely independently. In the 'on premise' configuration, it is sold on licensed basis depending on the number of users and applications.

Sedicii proves that a customer is not being impersonated, quickly, securely and reliably, **WITHOUT** any underlying sensitive personal information having to change hands. The user's identity attributes **NEVER** leave the device, browser or server. This reduces the burden of responsibility on the merchant whilst protecting the consumer. All sides win.