Real-Time Contact Centre Authentication

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

The exponential growth of the Digital Economy has created many challenges for businesses 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.

sedicii ZKP Verification

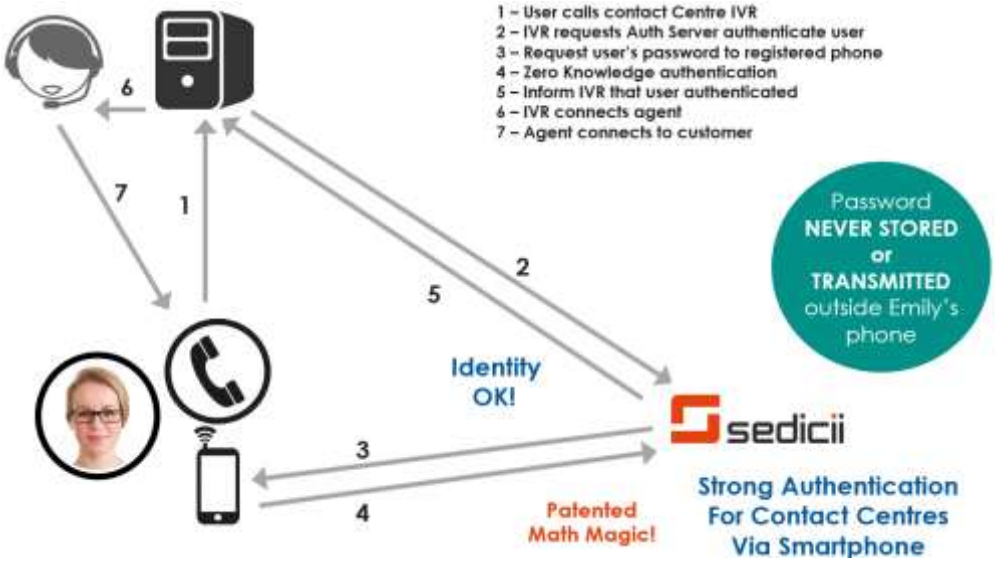
- ✓ Maximum Reliability
- ✓ Full Automation
- ✓ No Data exposure
- ✓ Fully GDPR/AML Compliant

The Problem:

Callers to a contact centre need to prove who they are before they can engage with an agent to discuss the reason for their call. Today, this is performed by the agent asking the user a series of security questions to which only the user is supposed to know the answers. The first 30-60 seconds of an agent's time is spent conducting this process with the customer which can be a cause of annoyance to the customer when they don't know or have forgotten the answers. It is also a source of inefficiency for the contact centre which could use this time for better, more productive purposes solving customer problems. The second half of this process is that there is no reliable and secure means for a call to a user initiated by a contact centre to prove to the user that the contact centre really is who they say they are. Sedicii has developed a smartphone-based service that will fix both of these problems.

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 Zero Knowledge Proof Verification engine (ZVE), the user can be authenticated without this signature being exposed or exchanged.



Sedicii Inbound Authentication for Contact Centres

Real-Time Contact Centre Authentication

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

Sedicii UK
20 Ropemaker St
London
EC2Y 9AR
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

online at:

Web: www.sedicii.com
Email: contactus@sedicii.com
Twitter: @GRRSedicii

The purpose of the service is twofold (i) to eliminate the need for an agent to authenticate a user through verbal Q&A for security questions when a user calls the contact centre and (ii) to allow a user to authenticate a contact centre caller when they receive a call from a contact centre. Both of these interactions are replaced by a digital interaction between the user, the Sedicii Authentication server and the user's smartphone. This will eliminate the time wasted by contact centre agents at the outset of any call as all callers are pre-authenticated while they are in the queue and not after they leave the queue and are talking with an agent.

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 a negative impact on customer satisfaction. Using the Sedicii Mobile Authenticator in a contact centre environment will:

(a) eliminate 30-60 seconds of an agent's time for every call that is handled. For large call centres handling 50,000,000 calls per year this could equate to a saving of up to 40 pence per call or £20 million annually

(b) eliminate the need to store any sensitive security questions and the cost of keeping that information securely stored

(c) increase call processing volumes by up to 10%

(d) reduce queue waiting time and subsequent call abandonment

(e) increase customer satisfaction ratings as calls can be dealt with faster and more efficiently

(f) provide bi-directional, mutual authentication for contact centre / customer 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.

Or, it can be provided in a cloud configuration where the same service may be shared by a number of organisations or services. In this configuration, the service is delivered on a transaction basis and managed entirely by Sedicii on behalf of the client enterprises.

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.