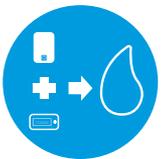# iDENtear

# STRONG MULTI-FACTOR AND MULTI-LAYER AUTHENTICATION FOR IDENTITY AND ACCESS CONTROL

iDENtear® combines strong security with convenience and ease of use as part of the design. iDENtear® is a self-sufficient and intelligent device that connects to smartphones, tablets, laptops or any other computing device without any physical connections. This makes iDENtear® an extremely unique, robust and secure device without any of the shortfalls associated with other authentication devices available today.

## MODERN SECURITY FOR MODERN LANDSCAPES
iDENtear® uses the latest Cryptographic standards that are robust. As this is a hardware device, it is not susceptible to risks commonly associated with Software based equivalents and does not have a reliance on the safety or security of the operating system on the computing device. iDENtear® is totally device agnostic.

## TRUE MULTI-LAYER SECURITY
iDENtear® is not just a Password Generator, it can integrate into Card Management Systems to provide Smart-card authentication. This means that current costs associated with purchasing smartcards, smart-card readers and device jackets and additionally, Hardware Password Generator devices are significantly reduced due to the multi-layer approach of iDENtear®.

## END USER CONVENIENCE
Trading off risk versus usability has always been a difficult task for any organisation. With iDENtear®, it is now possible to wrap Strong Access Controls and Authentication with usability. There is no need for users and customers to be juggling multiple security hardware devices or installing unnecessary and clumsy device "jackets", the iDENtear® device is simple and can be operated within your pocket or within your bag if you chose to do so. Operating the device is that simple!

## SECURE PROVISIONING AND ADMINISTRATION
One of the most unique things about iDENtear® is how it passes control to the organisation who are setting up iDENtear® devices in regards to ensuring complete secrecy of the material on the device and provisioning the device to end users. iDENtear® does not have the same problems as current Hardware Access Control device vendors have. We do not program Cryptographic seeds in the factory ensuring that the cryptographic seeds and secrets are how they should be, 100% secret.
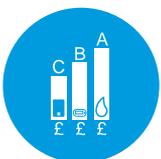
## COST EFFICIENT
iDENtear® has the ability to replace Access Control Hardware Devices, Password Generators, Smart-cards, Smart Card Readers including smartphone and tablet jacket devices. As well as the significant cost savings associated with replacing legacy technology, the device itself has been smartly designed to use the very latest components whilst keeping costs lower than other competitors. Our provisioning technology can ensure that iDENtear® devices can be recycled within your Organisation with complete new secrets or new end users.

## IN SUMMARY

• Hardware device that connects securely to computer devices over the air.
• Replaces traditional Password Generator Hardware Tokens
• Integrates to Card Management Systems and replaces Smart-cards
• No other hardware such as card readers are necessary
• For Remote or Local secure true two-factor authentication
• Very convenient for the End User and easy to use
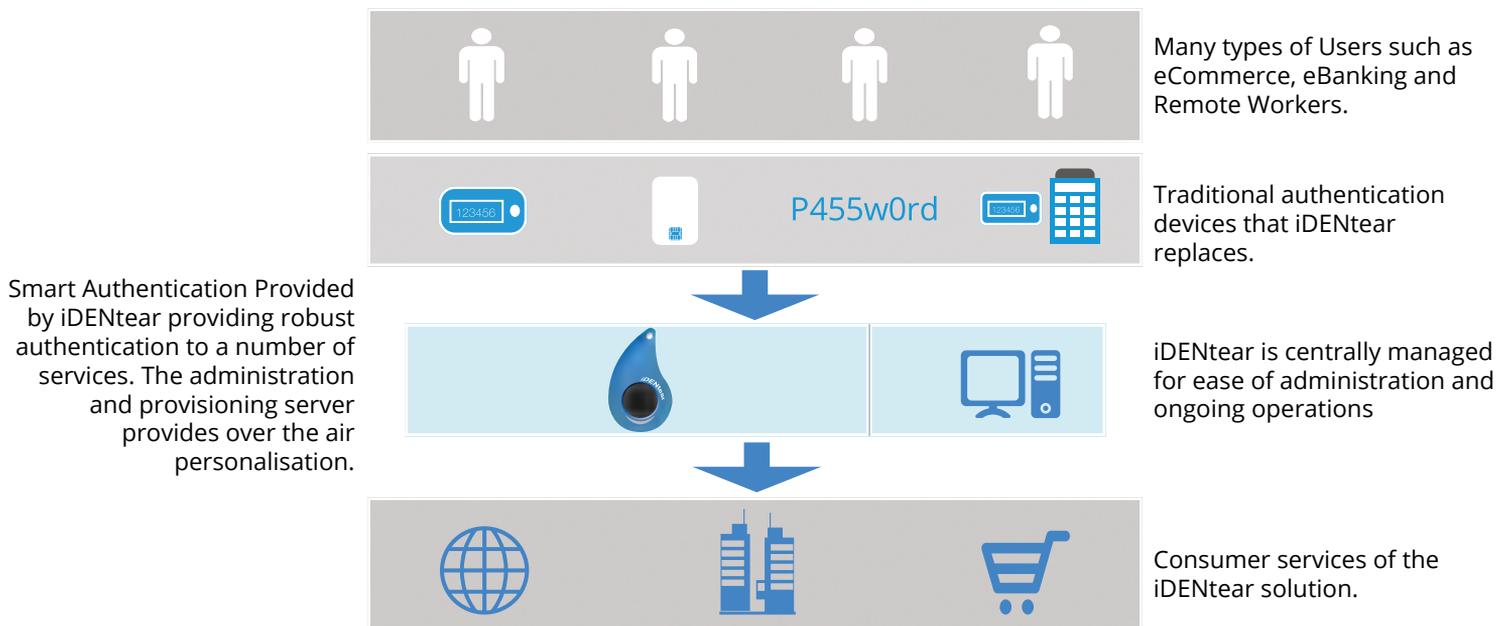• Cost efficient solution with real Return on Investment (ROI)

## WHY IDENTEAR?

Security conscious organisations that have spent considerable time and financial investment on ensuring their data is safe, often need to automate secure access to systems either on site or remotely to keep up with the demands of a dynamic and growing business within a fast market place, however, there are known issues with this especially in the current smart device era where security versus usability is normally a stand-off between IT Risk Departments and the Business, and this doesn't stop there. Demands from a more security aware customer and consumer base also require state of the art and convenient ways of accessing their services but without the hassle of owning multiple clumsy security devices but needing the assurance that their identity is safe, and clumsy security access to online systems and ebanking. Getting the user experience wrong leads to widespread complaints through App reviews and social media, damaging the hard work that organisations go through in regards to setting up "Convenient" online Services.

iDENtear ensures that the time and financial investments that organisations have made in securing their sensitive data is enhanced with a secure and robust solution that provides significant cost reductions against the more traditional hardware security password generators, Smart-cards and Smart-card readers with the additional benefit of being a better fit with modern smart device technology. iDEntear is designed to coexist with other security services and systems such as Public Key Infrastructure (PKI), RADIUS, Microsoft Active Directory and other security authentication vendors. They are also designed to work with a mobile population where convenience in their view is the number one priority. In essence, iDENtear provides:

• Strong True Multi-Layered and Multi-factored logical authentication
• Robust security device which can be trusted by the organisation
• Easy to use and very convenient to all end users regardless of their role
• Total control to the organisation ensuring secrets remain secrets.
• Seamless Provisioning from the iDENtear Authentication server
• Ease of Administration through the iDENtear Administration Server

## The iDENtear Use Case

Many types of Users such as eCommerce, eBanking and Remote Workers.

P455w0rd

Traditional authentication devices that iDENtear replaces.

Smart Authentication Provided by iDENtear providing robust authentication to a number of services. The administration and provisioning server provides over the air personalisation.

iDENtear is centrally managed for ease of administration and ongoing operations

Consumer services of the iDENtear solution.

| iDENtear Specifications | |
|---|---|
| Weight | 14 grams |
| Dimensions | 40.0 x 13.0 x 66.0 mm |
| Keypad | One-button |
| Time Source | Real-time clock |
| Supported Algorithms | SHA256, SHA1, ECDH, ECDHE, ECDSA, AES128/CBC OATH event (HOTP) or time (TOTP) based (on demand) |
| Battery | non-replaceable, lifetime expectancy 5 years |
| Environmental Attributes | Operational Temperature -20°C to +40°C Dust Proof & Water Resistant Tamper Evident |