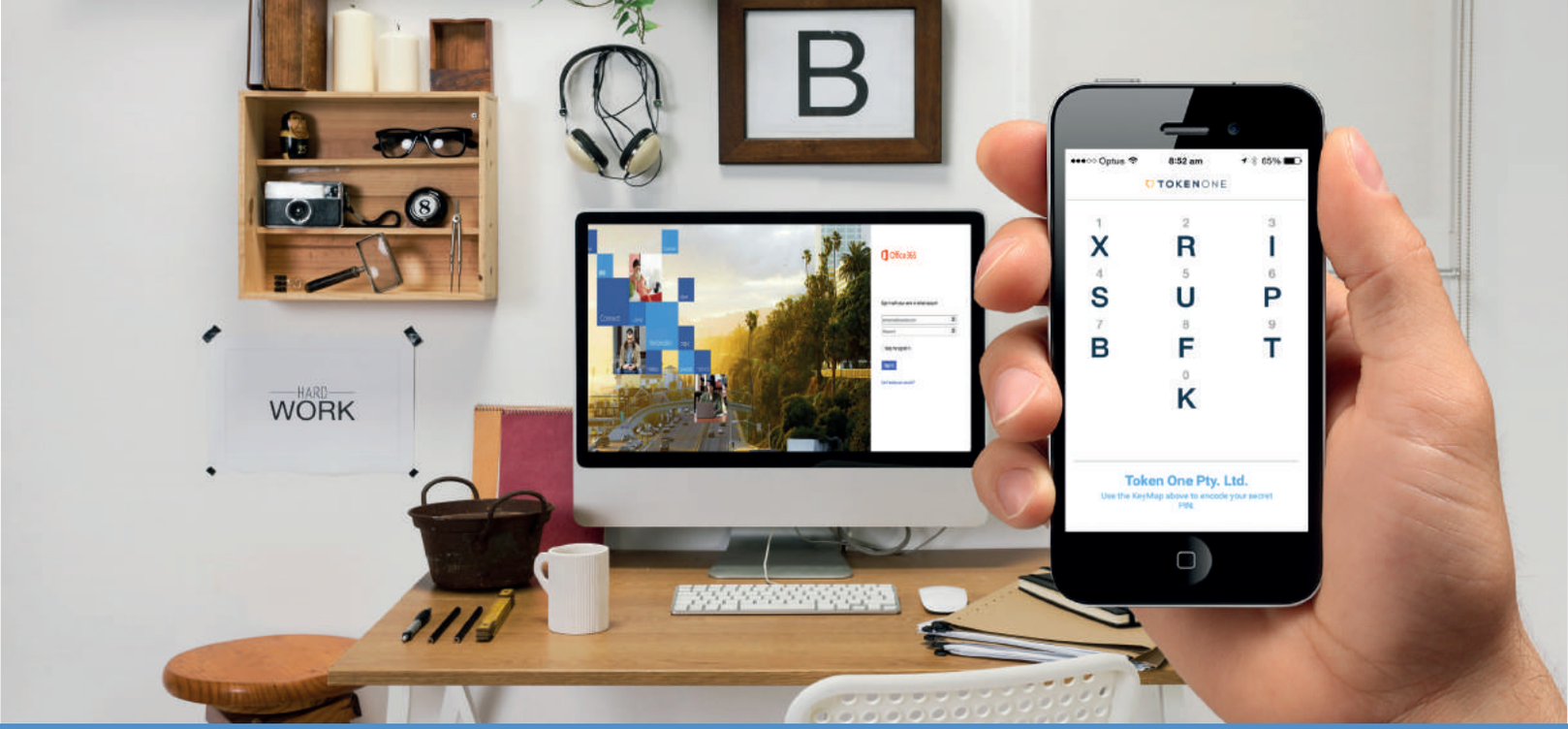
TOKENONE

Keeping Secrets Secret

Security, Privacy and Compliance at Scale



Keeping Secrets Secret

Security, Privacy and Compliance at Scale

COMPANY OVERVIEW

About TokenOne

TokenOne is a Cyber Security software company based in Sydney, Australia. TokenOne's internationally patented technology makes it easy for companies and their users to replace passwords, tokens and other forms of authentication security with a more cost effective, manageable and convenient solution that is highly secure.

Uniquely, with TokenOne Authentication a user's secret PIN is never entered, transmitted or even stored anywhere, except in the user's memory. Whether it's a hacker compromising the user's computer or a company's system administrator, no one else knows the user's PIN.

TokenOne Authentication solves the inability of passwords and other technologies to prove the real world identity of individuals on the Internet.

Currently it is very expensive or too risky for an enterprise to conduct many types of high value, sensitive or private business transactions and services online. This is largely due to both business risk and legal requirements of proving a user's identity.

TokenOne's unique and patented technology can be deployed rapidly and cost effectively by large organisations to the mass market of Internet and mobile consumers. TokenOne Authentication allows them to establish a provable link to each user's identity, but without the need for additional authentication hardware.

Unlike other security approaches that only focus on keeping anonymous hackers out, TokenOne Authentication also enables our enterprise clients to prove the identity of authorised users. This enables them to meet their legal and compliance obligations associated with proving who did what, when and why.

TokenOne "Keeps Secrets Secret!"

It's no longer just about keeping anonymous hackers out, organisations also need to be able to prove the identity of authorised users and who did what, when and why.

SOLUTION OVERVIEW

Deployment of the TokenOne Authentication Solution

TokenOne Authentication enables our enterprise clients to continuously prove the real world identity of their customers and users every time they interact with that organisation or service.

Registration & User Onboarding

Enable your users to prove their identity to required levels of identity assurance and link their real world identity to their digital identity.

Self-Provisioning & Management

Users self-register their mobile device as a secure token and create their own secret PIN.
Users manage their account, including PIN or mobile device re-registration.
Flexible process allows for existing processes of verification or biometrics to enable self-management.

Authentication

Strong 2FA & 3FA where all factors are strong.
Business rule driven red flags and multi layer authentication.
Continuously prove identity of users every time they interact with you.
Achieve non-repudiation, confident the user must be present to authenticate.

Proves User Presence

Enables legal compliance based on easily customisable ID verification and authentication rules.
Evolving client profiles based on online and real world changes.
Meet industry compliance and legal requirements.

Benefits for organisations

- TokenOne Authentication is easy to deploy (via the App stores)
- Cost-effective to deploy and manage - rapid ROI, low TCO
- Highly scalable en masse
- Manage users with existing IDM systems
- Password management costs a thing of the past

Benefits for users

- Simple and convenient for the user - ‘One phone, one app, multiple accounts and services’
- Self-registration with no extra hardware
- Highly secure and convenient
- Users securely self-replace their PIN, even if forgotten

TECHNOLOGY OVERVIEW

Features and Functionality of the TokenOne Authentication Solution

TokenOne Authentication allows users to easily verify their real world credentials and identity, register their mobile device as a token and create a secure and secret PIN. A user can complete all necessary steps in a way that enables your organisation to meet both identity proofing and legal compliance requirements. Users can also add credentials as required by your organisation's business rules.

Once users have a two-factor authentication account linked to both their real world and online identity, participating systems can:

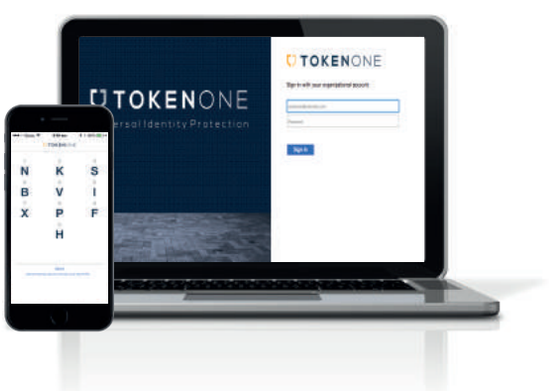
- more easily manage threats
- provide and track non-repudiated access at varying levels of identity assurance
- effortlessly capture and report information to meet legal and compliance requirements

Following registration, the simple TokenOne smartdevice app allows users to effortlessly convert their PIN to a unique and different alpha code each time they authenticate. With TokenOne Authentication the user's secret PIN is never revealed, even on a compromised machine. Moreover, through the mental process of converting a PIN to an alpha code, the user becomes a required part of the authentication process and this proves that the user was present.

Wikipedia (March 2014):
"In cryptography, a one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly…. However, practical problems have prevented one-time pads from being widely used"

TokenOne solves these problems.

```
ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDLCQT HZBSIZ IRZDYS RBYJFZ AIRCWI UCVXTW YKPQMK
CKHVEX VXYVCS WOGAAZ OUVVON GCNEVR LMBLYB SBDCDC PCGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL DWHPER UBSRUJ HGAAPR
CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE
```



Key Benefits:

- **No more passwords** - TokenOne Authentication doesn't require passwords, or password management, so is more secure and efficient.
- **Scale** - scales for mass numbers of Internet and mobile consumers.
- **Genuine strong two factor authentication (2FA) as both factors are strong** - TokenOne proves the presence of the mobile device AND the user and is one of the few mass market authentication solutions where both factors are strong.
- **Genuine strong three factor authentication (3FA)** - when combined with voice biometric and is deployable en masse.
- **No additional authentication hardware** - deployment of the TokenOne Authentication solution does not need any additional authentication hardware.
- **Not based on algorithm** - ensuring TokenOne Authentication is not vulnerable to someone cracking an algorithm and compromising multiple accounts and all associated services and infrastructure.
- **Complement existing and legacy architecture** - federated authentication and deployment across distributed or hybrid environments.
- **Patented technology** - based on an industry recognised uncrackable form of encryption (One Time Pad).
- **Zero Knowledge Password Proof** - a TokenOne user's secret PIN is never entered, transmitted and even stored anywhere. It remains a genuine secret.