Biometric Token Generation: 'Identifying an Individual Without Doubt'

WP: 0130-01

Table of Contents

Introduction

Usernames, Passwords, Security Tokens and PIN's etc. do not confirm that the person using them is the individual authorised to do so merely that they know the password or PIN. This is an inherent weakness and security risk when using any online service or application.

This briefing highlights the short comings of the identity processes commonly used today when accessing digital services. It introduces 'Associated Identity', which combines physical and a digital identity to make access **Frictionless and Fast, and prove 'without doubt'** the identity of an individual at point of access.

Match-to-Copy Weakness

Login systems rely on a match to previously copied and stored information e.g.

- PIN
- Passwords
- User ID's
- Biometrics
- Certificates

All these can and have been compromised by:

- Hacking
- Social Engineering
- Spear Fishing
- Malicious websites
- Email Trojans
- Internal security breach
- Etc

Ke2 &Associated Identity

The concept is based on a secure standalone physical identity token Ke2 and a token authentication service.

The aim is to prove a user's actual identity at point of access and replace the current reliance on trust that usernames and passwords are being used by the authorised person!

The core of the system is a unique and personal digital identity generated on a Ke2 token using a proprietary algorithm.

The ID is authenticated along with the token each time the ID is required and in effect will become a user's DNA for proving their digital identity.

The USP is an enabling technology for proving a user's physical identity "without doubt".
This is done by starting with the user who creates a simple, memorable and unique input (a combination of digital and physical inputs) only known to them (this will include digitised Biometric data in later versions).

The combination of this unique input and the device ID create an encrypted digital output that can only be created by the authenticated user and device in the same location.

Key features of this design are

1. The digital output is not stored anywhere, and can therefore only be created by combining the user input and device ID. This means that there is no single point of failure, as the digital output cannot be hacked, and 'Man in Middle' or similar attacks are prevented by using encryption.
2. Tokens are authenticated prior to any contact with online services (this creates an air gap to stop hackers seeing device activation).
3. A read only token that does not store any personal information, so nothing on the device for hackers to hack and totally safe if lost or stolen.
4. Tokens have unique heartbeats to prove the user is still present during connection.
5. Further authentication layers at point of use can be added to suit individual service provider or market requirements, and this can be done after the device has been issued to the user.
6. Use of the Ke2 can be stored to build a trust level for that ID.
7. The device can be used for any application enabled for its use.

Key Benefits

1. The digital output code can only be created by the user entering a digital/physical input known or enacted by that user.
2. The digital/physical input can be restricted to a unique biometric input provided in a unique way only known by the user. This prevents transfer of this input to other users (done willingly or under duress) and proves the input has come from that user.
3. The security platform and delivery is built once and used many times, making the delivery more reliable and more efficient.
4. The Ke2 hardware and core software are capable of being 'plugged in' to existing or challenging security environments with specific API toolkits.

5 The user only needs to remember one digital/physical input, there is no need to enter user name and password for each secure website/portal used.

6 Each user ID is controlled by a token, hackers can only challenge one identity at a time.

Business Benefits

- ✓ Instant confirmation of physical identity. (removes passwords etc)
- ✓ Ke2 simplifies and hardens existing login and user verification processes.
- ✓ Zero vulnerability from lost or stolen tokens to users or central services.
- ✓ One token for access to any online service and business resource.
- ✓ Scalable solution that can be easily integrated with existing systems.
- ✓ Corporate data access is controlled by actual, and trackable user identity.
- ✓ Reduces fraud.
- ✓ Cost effective and simple to deploy and use.

Flexibility

Partner organisations can develop processes for registering the use of the Ke2 ID on their systems e.g.

1. In person at a point where current trusted ID's i.e. Passports, Driving licences, Utility bills etc can be validated before activating and associating Ke2 ID's with user accounts.
2. Using the existing online registration process run by the service provider to add the Ke2 ID as part of the login.
3. Build trust models based on the user's Ke2 activation profile.

Typical use cases

- Banks: For proving customer identity for access and transactions online.
- Retailers: For securing access to regular customers.
- Banks and Retailers: securing links for online payments.
- NHS: Patient identity on and off line.
- Government: HMRC, DWP etc.
- MOD: Safe identity for personnel.

Technology differentiators

1. Ke2 is an **'Interactive'** personal identity token, with its own '**Intelligent'** read only processor.
2. Tokens can only be activated by one person i.e. the registered user.
3. Once activated, access is managed by the service the user is connecting to.
4. Each token has a secure point-to-point communications channel for challenge response and enabling safe messaging directly with the user.
5. Users can own multiple tokens connected to one ID for convenience, in case they lose one.
6. Construction of the chip in 3 layers means it cannot be reverse engineered as any attempt to dismantle it will break the chip;
7. Chip can be loaded with any algorithm for encryption; either a commercial one or a Government provided one.

Conclusion

The Ke2 identity technology provides a unique use case for personal security and identity management, namely a device for identity **associated solely with a single user** that is in effect disposable and immediately replaceable.

Delivers controlled user identity and access based on a user's identity, whilst removing stored personal information with all its vulnerabilities.

It enables accurate, fast and frictionless proof of a person's identity at point of access and interaction.

A Safe & Secure Digital Identity
'Without Doubt'