VeroGuard
Systems

VeroGuard Employee ID

The Challenges of Employee Identification

All organisations today are challenged with managing the digital identity's of their staff. With the growing number of IT systems and complexities of supporting legacy and modern platforms, user access management systems have developed complex layers of authentication in attempts to maintain control. From a security perspective 'getting it right' can often lead to extensive and ongoing management overhead of multiple platforms and solutions potentially creating poor user experiences, while 'getting it wrong' can mean data breaches and loss of credibility, not to mention significant financial penalties. In a time where the majority of significant data losses have occurred due to stolen user credentials, 'getting it right' is crucial.

The development of Access Management systems has moved in line with the technology platforms they support. The first era of Access Management was born in the late 90's to support on premises applications.

Around 2010, a new generation was required to cater for cloud applications which led to fragmentation where users are managed separately and redundantly in two environments. The third era is what analysts and industry see as the future: *Unified Access Management* - secure access management for all devices and applications, regardless of where they're hosted. Unified Access Management removes the need to maintain multiple systems and policies for users internally, on their own devices and accessing systems remotely.

With the current hybrid cloud and on premises IT environments of most organisations, maintaining control over who can access what is becoming a complex, costly and time-consuming task. This has led to layers of complex security and identity management being applied over many years, requiring staff to navigate the array of processes, ID's and passwords leading to useability issues and the requirement for staff to carry multiple ID tokens and devices. Despite many advances, existing technologies and architectures are simply not designed to manage the mix of legacy, on-premise and cloud systems. Single Sign On was seen as an early panacea to these issues but has largely failed as a function because existing architecture doesn't work across mixed environments.

94% of employees connect their work laptops to public wifi - *high risk of credential theft*

Complexity is the single largest issue of employees complying with cyber security rules

63% of employees use their work mobile devices for personal activities

2FA and other security measures are creating **friction** and dramatically increasing login times

Prevent unauthorised network access

Remove Complexity

Eliminate passwords

Reduce Costs

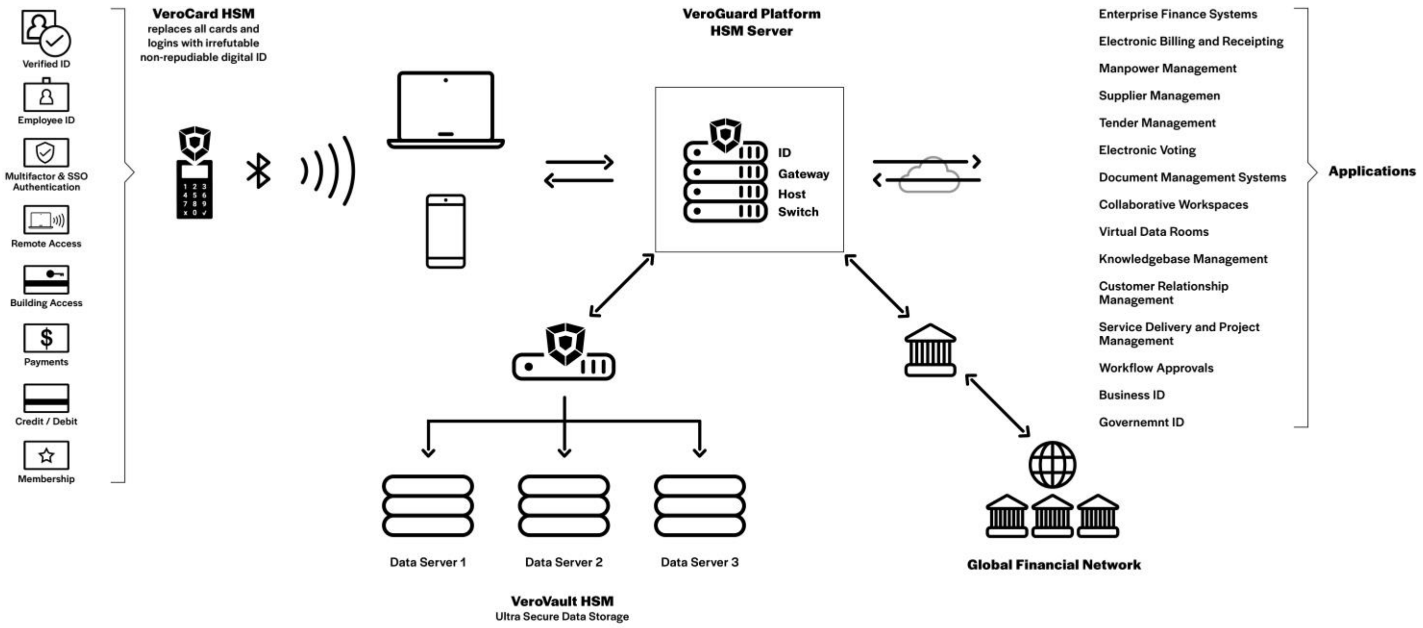
Improve Employee Satisfaction with Technology

A Unique Solution for a True Unified Employee ID

Employees typically have between two to five logins for different systems, a company expense card and one or more remote access tokens (hard or soft). All items are points of identity that require management and are sources of user frustration and potential identity theft. As people are increasingly mobile between multiple sites with each site requiring its own building access card (building owners choose building security systems), employees can often be required to carry multiple sets of company ID cards along with their system access credentials and authenticators.

VeroGuard's solution delivers a simple user experience that aggregates multiple ID credentials to one digital wallet with one PIN for multiple functions – not just identity or single sign on. This is a true unified ID that will work with any device or technology and removes the complicated steps or compatibility issues typical of existing identity and access systems. Users don't even notice they are being protected by military/banking level encryption security.

World's First Universal and Unified ID for Non-Repudiable Authentication, Privacy and Security



VeroGuard is the only solution which can address and aggregate all these items into one Digital Wallet (VeroCard) as a true unified staff ID experience combined with the level of security necessary to collaborate & prevent more cybercrime and ID theft.

VeroCard - Change the game on cybercrime.

VeroCard provides a unique digital ID allowing for anchored identification, single sign on, multi-purpose access and verification unified at the user and is interoperable across in-house, cloud and hybrid environments. ONE Identity ONE PIN for all access.

- Replaces ID Cards, eWallets, proximity cards (travel, building access) credit and debit cards, tokens, loyalty cards, licences, e-signatures and more.
- Higher security and simplifies integration.
- Simple, ultra-high secure messaging, collaboration (simplicity when extending inter or intra network collaboration involving secure transactions and data flows. Everything can operate at a high assurance, ultra-secure level across extended open networks). Verifiable identity across the internet, highly interoperable and compatible with most applications and operating systems.
- Transformational security and interoperability for networks.
- Best of Breed data protection for any system exposed to the internet (directly or indirectly)

The VeroGuard secure access platform is a highly scalable distributed platform which provides a Hardware Security Module (HSM) to HSM level security connection between a user and host system or application with true non-repudiable identity – because no one can pretend to be you with the VeroGuard solution.

A Single Secure Platform, VeroGuard's Employee ID solution can provide:

✓ A unified staff identity and multi-function experience that is interoperable across an entire organisation
✓ Single sign on for all applications with one Card and one PIN
✓ Secure remote access and Device access
✓ A new converged identity and security architecture designed to traverse between closed and open networks, modern and legacy environments

The VeroGuard platform **removes** the need to buy technology like:

- Federation software
- Single Sign On software
- Remote access software and tokens (hard or soft) eg: RSA, Citrix
- Digital PKI certificates
- Some dedicated telco communications because it can work securely over the internet
- Some third-party DMZ security network zones (infrastructure) because trusted connections are possible

Value Added Services: unique value with extra functionality embedded within the platform that can be switched on as required and configured when Organisations desire. Some of those functions are:

- end-to-end encryption secures the whole transmission at HSM level of security
- secures the end user's activity from any device and can secure the device (PC, tablet or phone)
- security for privileged or top-secret level embedded
- building access (NFC tap)
- real time authorisations, privacy, workflows
- contactless payments – can store multiple cards
- Business
- Citizen ID
- blocks all unknown protocols from entering systems

VeroGuard's solution works with any Bluetooth enabled smartphone, PC or tablet, which removes compatibility and security issues of having digital identity in a software application; which can cost organisations millions of dollars to design for the vast array of device and application technologies. The "out of band" nature of the VeroCard means it is quick and easy to deploy, maintains the ultra-secure techniques and aggregates all cards and tokens into one digital wallet.

What has VeroGuard Systems Developed?

VeroGuard has developed a solution to the problem of not knowing who or what is at the other end of an online transaction, and therefore the authenticity of the interrogation, communication and associated data. VeroGuard provides this surety via a non-repudiable Digital ID and authentication platform, capable of irrefutably identifying humans or machines – making it applicable to any online interaction. VeroGuard combines this non-repudiable ID with hardware encrypted protection for data in transit and at rest in the cloud.

VeroGuard provides a single gesture, out of band, multi-factor authentication solution based on existing proven bank to bank protocols applied as a first of its kind to the cloud and can provide hardware encrypted and verified security access across platforms regardless of device, network or location.

VeroGuard's system can provide the necessary infrastructure to extend protection to any organisation, secure communication between parties, create a trusted environment and to reduce incidence of attacks based on identity or credential loss.

The VeroGuard solution has three main elements:

1. **Portable non-repudiable Digital Identity that is unified, universal and irrefutable**. A single platform that authenticates people and/or machines over the internet using ATM authentication and bank to bank level communications.
2. **Ultra-secure cloud communications** combined with simple API's to enable hyper convergence for online services.
3. **Ultra-secure storage**. VeroGuard has partnered with Data61 (CSIRO) to also secure data at rest in the cloud, to take cloud data protection to above protected levels leveraging a multi-server splitter and the non-repudiable identity of the actors.

How does VeroGuard address Cyber Security issues?

Solution	Benefit	Issues Addressed	Online & IoT Security
Portable non-repudiable Digital Identity	A single platform providing Unified, Universal and Irrefutable Identification	**Prevention** Bad Actors cannot access devices **Universal** Identity unified at the device – not the system	Guarantees identity of persons authenticating to an application, or machines on your network with bank to bank level security
Ultra-secure cloud communications	Simple API's to enable integration of any online service	Enables hyper convergence for online services, as the identity layer is already catered for	Guarantees data transmission is secure and ensures communications can only take place by verified actors
Ultra-secure storage	Lifts cloud data protection to a completely new level (above protected)	Data at rest is not subject to being accessed by a single attack	Files are split across multiple storage solutions and each component is encrypted, meaning multiple successful attacks would need to be accomplished

What are the components of the VeroGuard Solution?

VeroGuard is a unique technology that enables online authentication and encrypted transmission across fixed and mobile networks with same level of identity security as the ATM network. VeroGuard delivers non-repudiable secure open internet-based login which can be integrated into any environment. It has proven significant defensive security using multiple layers, using an anchored ID and multi-factor authentication for best of breed digital identity verification, suitable for use by employees and clients.

The VeroGuard platform serves as a central exchange enabling authentication of users and devices online. Once authenticated ultra-secure communications and storage options can also be provided to create trusted member ecosystems, opening new possibilities for collaboration amongst members. The core components of the solution are:

VeroGuard: The central platform providing HSM to HSM level authentication, interoperability and switching services, managing the verification of identity, multi-factor authentication and secure VPN to secure shared services such as cloud storage and email. VeroGuard can protect machines and users equally on a single platform providing a solution to protect IoT or machine-to-machine interfaces, protecting and verifying end points, applications, communications and data with hardware encryption and encrypted packet splitting.

VeroVault is a secure cloud and email service which can be connected to a range of cloud providers, delivering HSM to HSM level secure access and data secured in the cloud at rest with hardware encrypted multi server packet splitting with storage able to be across providers.

VeroCard: An HSM level Digital Wallet for users to manage secure identity access, authentication and transmission. This card is tamper-proof and designed to connect to Bluetooth devices on any operating system. If lost, the card has no accessible data contained and can be remotely disabled.

The VeroCard has been developed to be the ultimate in personal security of the most precious personal details as well as protection of all online activity. VeroCard is the personal hardware that enables the VeroGuard system, providing personal ID security and privacy control, it is a credit card sized tamper proof “Black Box”1 Bluetooth device. VeroCard provides an easy and secure point of entry for all sensitive information protected with a PIN.

VeroCard enables the user to access websites, applications, cloud storage or payment systems through a secure server, with real-time authentication back to the VeroCard that the user holds in their hand.

VeroMod: HSM level embedded Digital ID and encryption for Machine to Machine interfaces. It is a secure digital identity that can be embedded into IoT connectivity to irrefutably identify the device and provide encryption for the data. VeroMod can be embedded into devices or connected in-line and in conjunction with VeroGuard which provides HSM to HSM authentication and verification of device identity. The VeroMod can be used to secure any type of device and handles the processing load for cryptographic calculations meaning the IoT devices are not impacted by the security workload.

1
2
3
4
5
6
7
8
9
X
0
✓

[1] “Black box” security refers to devices which contain Hardware Security Modules (HSM) and encrypt communications based on processes where the security keys are maintained within hardware that safeguards and manages digital keys for strong authentication.

Extended solution

VeroGuard delivers unified, universal digital identity that can be re-used and recognised without extra infrastructure for multiple applications including systems access, physical building security, secure document transfer, authorisation of transactions and payments.

The VeroCard is a credit card sized device, secured with a PIN, that you can use to manage your digital identity through the secure VeroGuard system.

VeroCard – when used as a Digital Wallet has the capacity to store more than 100 cards securely within its tamper proof black box.

VeroCard could be used as both your business (authenticate onto your corporate network) and personal ID (authenticate onto your personal email, government websites, banking and online shopping).

It could be used to store important identity information such as digital driver's licences, other licences or permits and frequent flyer cards. Enter your payment cards into your VeroCard and use it to tap-and-go and pay online – especially with real Debit online.

VeroCard can also be used like an EFTPOS to receive payments from others

The best part? VeroCard provides real-time authorisation notifications — so if someone tries to use your bank or credit cards, or to log in to a site using your details, you simply don't enter the authorising PIN, with this system you are totally protected against unauthorised use.

VeroCard is totally secure:

- ✓ Uses a single unique pin.
- ✓ Can't be skimmed, can't be tampered with.
- ✓ Locks out anyone who doesn't know the pin.

VeroGuard Schematic How does VeroGuard address Cyber Security issues?

Feature	Benefit	Description
Hardware Encryption	Private keys and are never exposed to software where they can be harvested or broken by malware or applications.	HSM to HSM encryption for communications based on processes where the security keys are maintained within hardware that safeguards and manages digital keys for strong authentication. This methodology means that the encryption can't be broken or associated if intercepted. Devices are tamper-resistanrt and provide out of band multifactor authentication with a single gesture.
Hardware Token with Single Gesture, Multifactor, Out-of Band Authentication	Provides a separate layer of security for the strongest possible authentication. The VeroCard provides this solution seamlessly for each login with the user only required to enter their PIN. Uses a single unique pin. Can't be skimmed, can't be tampered with. Locks out anyone who doesn't know the pin.	Out-of-band refers to authentication that requires a verification method through a separate channel.
Portable	Can be used to authenticate access to any online system or encrypt communications end to end between devices.	VeroGuard is a single platform that authenticates people and machines over the internet using bank to bank level security. An ID is anchored to the user and verified on a separate identity solution, enabling the Digital ID to be re-used for any system you wish to bring online, or keep terrestrial.
Ultra-Security	No meaningful data is associated with identity captured or sent, and there is NO KNOWN SOURCE OF THE KEYS.	Keys are stored in Hardware Security Modules (HSM) and never exposed to software, providing ATM like authentication which cannot be broken or associated if intercepted. New key pairs can be exchanged with EVERY transaction..
Flexibility / Interoperability	Any OS, any device, any system	VeroGuard is agnostic to operating system and device types allowing enabled devices and associated servers the ability to participate without significant changes to applications.
Identity Guarantee:	Know who is at the 'other end'	VeroGuard uses a non-repudiable, out of band, multi factor means of authentication which can be applied to both machines and humans and makes every authentication verified.
Information protection:	Ultra-Secure encrypted tunnels and cloud storage	VeroGuard can provide an encrypted tunnel for communications irrelevant of the carriage. VeroGuard provides the most secure, unbreakable cloud storage solution available but able to be applied to existing services.
Low Cost	Low cost solution, and can remove the need for other identity solution and integrations	
Scalable	A single Digital ID is reusable across any online platform.	
Reduces Complexity	Removes the complexity of building security into digital platforms	