VeroGuard Systems

VeroGuard Citizen ID

A Solution to the Citizen Identity Challenge in a Digital Economy

The transition to a digital economy requires a trusted, efficient and unified secure method for accessing government services. A VeroGuard Citizen ID seamlessly connects citizens to government services and stops unauthorised access, providing absolute trust between citizens and government. Our platform not only switches between government and corporate applications, but is designed to certify into existing financial networks to utilise existing schemes and settlements at cardholder present level online. It automatically complies with banking identity frameworks and existing retail payment terminals.

Citizen ID allows for easy and ultra-secure access to online services for any level of government. It is a universal solution that enables secure online proof of age, online voting, E-health data, E-Prescriptions, digital public transport wallets, event ticketing and so much more.

The Challenges of Citizen Identification

Governments worldwide have a duty to protect their citizen's identities and personal data. Constantly looking at new ways to provide convenience for their citizens, more utility and access to services, governments must also ensure privacy is unquestionably protected. In the face of recent public data breaches around the world, this is the key challenge to guarantee a program of digital transformation does not end up opening more gaps for criminals to exploit.

Needing to show your identity documents in person is the biggest barrier to government services being available end-to-end online. Where proof of identity is required before services can be established, current practices necessitate the collection, verification and storage of an individual's identity details, a process which is cumbersome and exposes both the individual and the organisation to undue risks.

This process is repeated every time a citizen wants to begin a relationship with a new department, agency or service provider, and each organisation must verify and retain a copy of the same identity documents. Citizens interact with government at multiple levels from registering births, deaths and marriages, to filing tax returns, obtaining a driver's licence or enrolling a child at school, and each interaction requires identification.

Globally, governments are seeking solutions to this situation and enabling a national digital identity system which allows users of government services to get more done online at a time and place they choose (i.e. at home and after normal business hours), is a significant and potentially (in this age of cyberattacks) daunting step forward. The purported benefits of a digital citizen identification scheme are clear – faster and simpler access to government services for citizens and businesses, and for governments efficiencies and cost savings. A digital citizen identity should also offer citizens more security over their identity and a consistent user experience when dealing with government, as well as close off many of the avenues to defraud the state with duplicate identities through the social security, health and tax systems.

Further, a digital citizen identity should be extensible to combine multiple physical identities, incorporating government issued cards and licences, and be used by enterprise to simply and easily verify customers. Some governments have already implemented a smartcard based digital citizen id and are reaping significant benefits. Estonia's digital id is the most highly-developed to date incorporating proof of ID with travel within the EU, health insurance, e-prescriptions, public transport, voting and taxes. According to the Estonian government, 99% of government services are now available digitally, with only marriage, divorce and buying real estate requiring physical presence. Further they estimate savings through this program of 800 working years annually – or 2% of their GDP.

Most citizens have at least 4 pieces of government issued physical identity documents, and can easily have up to 10.

Having to produce your physical ID is the No. 1 blocker of government service provision over the internet

A digital citizen ID can save time and effort for all parties when interacting online ***and*** offline

"Tell Us once"
Verify a citizens identity and leverage across the entire government ecosystem and into enterprise

Absolute Trusted Identity

Enable Digital Transformation of Government Services

Crack down on Duplicate Identities

Reduce Costs

Improve Citizen Satisfaction with Technology

Unshared Solutions – a Common Road Block

In general, governments structure themselves in multiple layers to service federal, state and local community needs, and it is common for citizens to have multiple identities with each level of government and with various departments. Many Government entities are largely independent organisations responsible for their own systems and policies, which creates widespread issues of significant variation in data that is being captured and quality of the data. Sharing of information across organisations is therefore extremely difficult and fraught with risk, due to the lack of a common identity. Many solutions have been investigated in the past including standard platforms, shared services and federation – none of which have been deemed to be suitable.

As it is not feasible for each department and agency to utilise the same platforms or software, the requirement for a universal identity layer to enable the digital transformation which is sought by governments will not go away. A universal and unified digital id can provide an identity layer across entire ecosystems, breaking down the barriers of integration and providing increased utility.

The current hybrid cloud and on premises IT environments of most government organisations and maintaining control over who has access to what data is becoming complex, costly and time-consuming. This complexity has led to layers of security and identity management being applied over many years, requiring citizens to manage their individual profiles across multiple systems and requiring citizens to navigate the array of processes, ID's and passwords, leading to reuse of credentials and potential identity loss.

Security and Privacy

Concerns around security and privacy are common, people are becoming more aware of the need to protect and safe-guard themselves against breaches. Individuals are worried about personal details being held centrally and accessed by multiple government agencies, and with the recent well-publicised leaks by both private and public sector organisations, public anxiety on this topic has escalated. For citizens, this correlates to being able to protect and own the data that the government holds and control which departments and agencies can have access to their data.

To citizens these are significant concerns when considering a unified identity. Additional concerns have been raised that a unified citizen identity would enable governments to gain insights into citizens everyday lives, tracking and monitoring their every move. This situation is akin to a central database approach, where all transactions and interactions are mapped back to a single point.

In a universal and unified identity approach, identity becomes the central factor and user accounts on department and agency systems including databases could become de-identified. Example: a citizen's utility account shows a usage threshold at an address in their jurisdiction has been met and the council wants to send out a new bill for the next period. The citizen account is linked to ID: BE23-ED43-3788 with no name, age, sex or other personal information attached. In generating the message to the citizen, an API call could be made to the central bureau of ID to collect the necessary name and email address for an automated communication. Details of the communication are stored without the identifying details.

> *Is it more secure to have your identity details spread across multiple systems or secured in one central location?*

The Solution

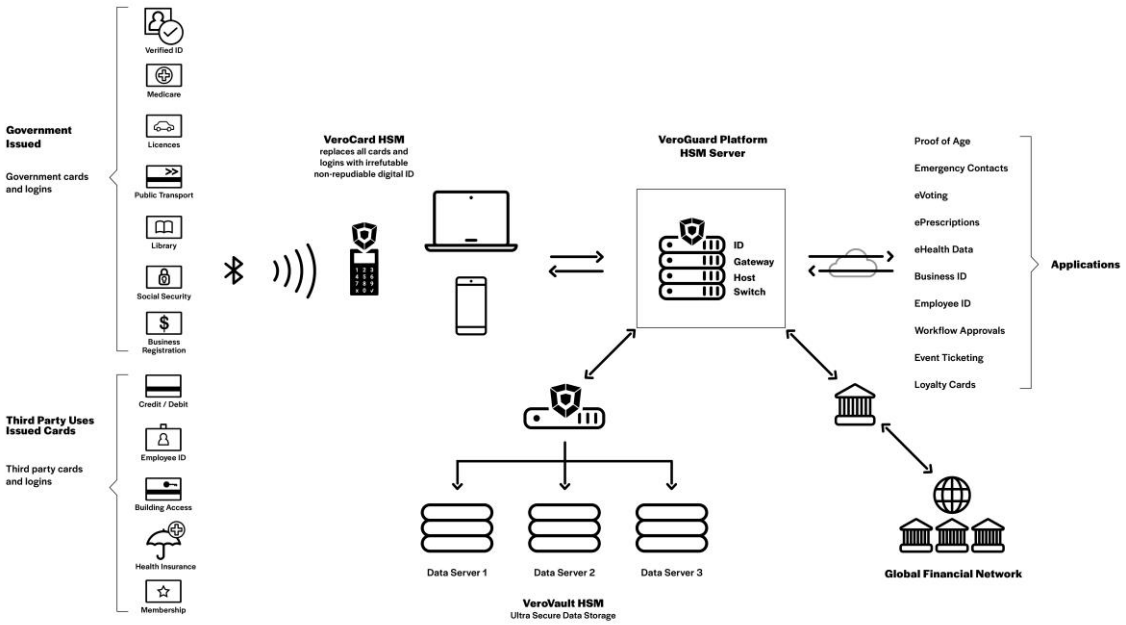
VeroGuard's secure ID platform enables a single validation of a citizen's physical ID to be leveraged across the internet anywhere anytime. VeroGuard's universal, unified and non-repudiable digital ID, is secured in a tamper proof hardware device which can authenticate a user's identity irrefutably without having to provide any further form of identification, and without sharing any information the individual chooses not to share with that entity.

As a platform, VeroGuard can provide the Digital ID service and make it available to any organisation to integrate. Once integrated with VeroGuard, any government department, agency or business can accept the ID provided by the VeroCard - *confirmed by out of band*[1] *multifactor authentication* - is proven and **Trusted.**

Absolute Security - Single gesture out-of-band multifactor authentication ensuring an individual's identity cannot be accessed by anyone other than the individual.

- **Ask Us Once** – Enables reuse of identity and other personal data across government platforms, so citizens need to enter/update their details once.
- **Absolute Privacy** –The citizen can choose to allow an entity access to their details, ensuring that their privacy is always protected.
- **Remote Provisioning** – Once established a VeroGuard Citizen ID can have additional attributes provisioned or revoked in real-time remotely (e.g.: adding a Heavy Vehicle licence), removing delays and costs in production of physical cards and their distribution.

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 government, enterprise and private identities into one Digital Wallet (VeroCard) as a true unified citizen ID experience combined with the level of security necessary to ultimately protect private information and & prevent cybercrime and ID theft.

[1] Out-of-band refers to authentication that requires a secondary verification method through a separate communication channel. For example, where system access requires both a standard username and password, as well as making a telephone call from a preregistered number.

A Unique Solution for a Universal Citizen ID

Citizens typically have between two and four pieces of physical identification provided by their government, but it would not be uncommon to have 10 or more. Starting with a Birth Certificate and (in Australia) a Medicare card, add to that a driver's licence and a passport and these four items would be the basis of proof of identity at government service locations and private institutions such as banks.

The smartcard solution rolled out in Estonia has provided a significant uplift for citizens and the state, however this implementation has not been without issue. A flaw in one of the security chips effectively enabled the private key to be calculated

from the public key, meaning an attacker could impersonate an identity. Other similar technologies based on Public Key Infrastructure (PKI) will have a limited lifespan with nascent quantum computing technology said to be able to break this encryption in minutes.

VeroGuard's solution delivers a simple user experience that aggregates multiple ID credentials to one digital wallet with one PIN for a unified and universal identity applicable across an entire government's platforms. 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.

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, creates an absolute e-signature and more.
- Higher security and simplifies integration.
- Simple, ultra-high secure messaging, collaboration. 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 solution 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 Citizen ID solution can provide:

- ✓ A unified citizen identity and multi-function experience that is interoperable across any government systems and can be harnessed by the local business ecosystem.
- ✓ Single gesture multifactor authentication for all ID requirements with one Card and one PIN
- ✓ A new converged identity and security architecture designed to traverse between closed and open networks, modern and legacy environments

Value Added Services: unique value with extra functionality embedded within the platform that can be switched on as required and configured when government and/or users desire. Some of these 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)
- building access (NFC tap)
- real time authorisations, privacy, workflows
- contactless payments – can store multiple cards
- Business ID (see paper on Business ID for more info)
- Employee ID (see paper on Employee ID for more info)
- 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 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 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?

Portable non-repudiable Digital Identity	A single platform providing Unified, Universal and Irrefutable Identification	**Prevention** Bad Actors cannot enter a system. Phishing attacks are eliminated **Universal** Identity unified at the user – 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, an anchored ID and multi-factor authentication for best of breed digital identity verification.

The VeroGuard platform serves as a central exchange enabling authentication of users and devices online. Once authenticated ultra-secure communications and storage 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, protecting and verifying end points, applications, communications and data with hardware encryption and encrypted packet splitting.

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"[2] Bluetooth device. VeroCard is easy to set up and easy to use, access websites, applications, cloud storage or payment systems through a secure server, with real-time authentication.

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. Connects and protects regardless of network connectivity including RJ, CAT, Cellular (2/3 /4/or 5G) WiFi, BPL/PLC.

VeroVault is first of its kind and best in class Secure Cloud Storage, Retrieval, Sharing and Collaboration for Documents and Data.

VeroVault seamlessly leverages multiple existing best in class storage providers by splitting data into encrypted packets and storing them across multiple providers and locations. These include Amazon Cloud Storage with AWS, Microsoft Azure Storage, Google Cloud Storage, IBM Cloud Storage, etc… This provides benefits such as:

- Data Store and Retrieve Striping
- Higher Data Security by distributing storage with hardware-based encryption
- Easily add or remove suppliers

Stored Data is also secured by encrypting using a Hardware HSM with each Data Packet encrypted using best practice AES under Elliptic Curve encryption.

Users can only access VeroVault via VeroGuard using their VeroCards, affording the highest level of secure, traceable, and un-repudiable identification-based authentication.

VeroVault gives businesses and users sharing, collaboration and secure email in an unparalleled secure cloud storage experience.

[2]"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.


1 2 3
4 5 6
7 8 9
X 0 ✓

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. When used as a Digital Wallet it 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 is a full EFTPOS certifiable device (ISO 8583/AS 2805 and PCI PTS 5 and above), and as such can receive payments from any financial regulators participating cards (tap and PIN)

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.

Why is VGS a revolution in Online and IoT Security?

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	

VeroGuard Systems Pty Ltd
ABN 25 617 573 001

P / +61 (03) 9558 3090
admin@veroguard.com.au

veroguard.com.au