Modernising Business Registers Program (August 2018)

A submission in response to request for feedback

Prepared By:

Ross Peacock, Kane Parker and Varun Pant from EnterpriseCreativeCloud.

About EnterpriseCreativeCloud:

The EnterpriseCreativeCloud team have been actively involved in the development and successful delivery of modern digital government services for use by small business. These services span local, state and federal government transactions. Our team has experience in practical design and implementation of new and complex digital government services, identifying and quantifying benefits and value for multiple stakeholders, together with a detailed understanding of the challenges and opportunities for government and small business when transacting with government. The team have over 12,000 hours of experience in specifying, designing and building digital solutions including setting up and running highly successful Proof of Concept (POC) trials with government. Trials which encompass establishment of digital services and solutions across desktop, tablet and mobile devices and the planning, design and introduction of new local and state government operating models using best practice agile and change management delivery approaches. EnterpriseCreativeCloud continues today to work with various state and local government clients on the introduction of modern, innovative digital services.

Our Passion:

There is enormous scope for positive change in how government supports small business. The outcomes of the Modernising Business Registers (MBR) program are critical to establishing new digital foundations that will underpin the future digital services introduced by all government agencies. The EnterpriseCreativeCloud team are passionate about supporting real change in how modern digital services evolve with focus on collaboration and user-centric solutions to support small business and government to transact in meaningful ways to achieve efficient business services with better outcomes.

Our Work with Government:

Leading the entire NSW Easy to do Business (EtdB) program from initial start-up to maturity (24 months) and the associated collaborative work with the Australian Government, Department of Industry, Innovation and Science (DIIS) with respect of the implementation of new Business Registration Service (BRS) for use by small business start-ups. This EtdB work spanned 128 NSW Councils, 13 state and federal agencies and resulted in the introduction of new, standardised ‘tell government once’ digital services across the 3 levels of government.

Examples of the work we are involved in

Click to see the Nine Network EtdB Video

Design Question	Consideration	Proposed Strategy	Target Outcomes
LEGISLATION What legislation is required to allow for the modernising of business registers? **Q1.** What flexibility would you like to see introduced into the relevant legislation?	**Our Response** Business to government transactions (use cases) vary from simple to complex. The ability to correctly identify and digitally verify related business entity, transactions and ownership remains a challenge when introducing new government digital services for business. The introduction of the Director Identification Number (DIN) will enable better tracking of directors of failed companies but also will provide a significant opportunity to make it much easier for businesses to navigate government requirements by simplifying the design and introduction of new digital government services for business. For this reason, DIN will be used by local, state and federal government agencies to improve digital services, the customer experience and internal customer service processes. The introduction of DIN should reduce (if not help eliminate) current reliance on 'wet signature' when	**Our Response** Ensure that the legislation addresses the following: - A. Local, State and Federal government agencies have access to all DIN information and can digitally validate the DIN against ABN and Company TFT(s). B. DIN numbers should be constructed so that they include relevant self-check features (i.e. checksum) to reduce the opportunity for false keying during entry in digital forms. The legislation should mandate that all applicable government agencies adopt the self-check features during data entry. C. Anti-fraud strategies should be adopted to reduce the opportunity for intentional misuse. DIN should include a validation number only known by the Director and not held by government except for short term validation of the DIN. This would be in the form of a PIN number or equivalent with PIN numbers available (and updatable) via self-service within GovPass.	**Our Response** 1. Ensure consistent implementation and use by local, state and federal agencies 2. Improved mechanism to avoid human error 3. Improve the mechanism to validate ABN, DIR and legal entity via ABR API services 4. Reduce opportunities for fraudulent use 5. Support court decisions in relation to actions with respect of Directors rights and obligations 6. Avoid DIR misuse by private enterprise. Maintain the privacy of the individual with respect to non-government entities. 7. Ensure DIN and GovPass work together to provide effective and efficient support for business transactions with government.

	transacting with government. Legislation should be focused on supporting and encouraging whole of government implementation of DIN in conjunction with other initiatives such as GovPass. Government agencies must have the flexibility to use DIN to build new, modern fit for purpose digital business transactions and supporting customer service functions.	The online public version of the DIN register should incorporate lessons learned from existing DIN deployments and not enable identity theft. D. DIN should be revocable for the equivalent period of time that a Directors rights have been removed (blacklisting of the DIN for a period). E. DIN should include a validation number only known by the Director or Authorised Officer and not held by government except for short term validation of the DIN. This would be in the form of a PIN number or equivalent with PIN numbers available (and updatable) via self-service within GovPass. F. DIN data should not be available to private enterprise, except via use of API validation services. Private enterprise should be barred from holding the DIN number or any associated PIN. They should instead only receive an approved 'validation response', transaction number that is traceable back to the enterprise	

Initiative 01 for Consideration	Ensure DIN can be used by government to construct/validate accurate ABN, TFT and DIR relationships, even in the most complex structures. DIN APIs for use by agencies to support this initiative.
Initiative 02 for Consideration	DIN number to include a self-check checksum. Mandate agencies to use this feature of DIN
Initiative 03 for Consideration	Provide business owners with a PIN (unique to each individual) for use with DIN for electronic confirmation. Support via legislation. Allow business owners to update their PIN via GovPass.
Initiative 04 for Consideration	Ensure private enterprise can request DIR, ABN, TFT type confirmation via API's but ensure they cannot hold this data for data mining purposes. DIR's primary purpose should be for government use and to reduce digital transaction complexity for the business owner. The business owner could either hold or access all DIN information held by government. In order to transact with the government, the business owner could encrypt the transaction information using their private KEY linked to DIN, and government can validate the information using their public key via a common website.

PTO

Design Question	Consideration	Proposed Strategy	Target Outcomes
ENHANCED REGISTRY SERVICES How we can enhance the services offered and improve the user experience? **Q2.** What modern services should be provided for Australia's business registers?	**Our Response** Registry services should solve problems for business as well as government to ensure widespread adoption and support within the business community and continuous use by business beyond initial registration. The value of any government register is measured by the value to the holder of the registration. New registration data quickly becomes old data and of little value if not kept up to date (onus on the Business Owner to keep the data accurate, as it will be matched against other authoritative sources held by the Govt). Business holders of registrations such as a DIN must have an easy means to update their information and consistent way(s) of updating this information via various government channels. A standard API should be available to local, state and federal agencies that allow the business to update their register whilst in the process of transacting with the agency and without leaving the transaction.	**Our Response** A. Build registration update services for government agencies that can be re-used without having to return to the federal registration site for update. B. Ensure the method of update is consistent and provide the means to allow business to set reminders to update their registers on a quarterly or yearly basis. C. Ensure updates are only completed by authorised people via the use of secondary identifiers (equivalent to unique PINS). D. Ensure the solution supports and manages authorised people to update business registry information in terms of their identity, role and responsibilities.	**Our Response** 1. Ensure consistent implementation, use and support by local, state and federal agencies. 2. Encourage regular updates to the register as business goes about its business. 3. Consistent and regular digital interactions by business and the introduction of tools to remind business to update their information. 4. Registrations updated, by the right people to the right time and having the right authority. 5. Ensuring a positive sentiment and on-going use of services by providing continuous communication on benefits of using registry services both internally within government and externally to business users and community, considering opportunities for joint media releases with local and state agencies.

	Agencies should be encouraged to implement such services in their design. Modern Registry Services should encompass plans to expand across the wider business eco-system to ensure that as business transacts with government, sufficient touchpoints exist via government and non-government channels to ensure there is an opportunity for business to update their registers as they go about their business. In summary, a federal focused DIN register that looks to solve some federal agency problems (e.g. Identifying phoenix activity) rather than encourage and support wider adoption across all agencies would in fact do little to enhance the future delivery of government services to business.		
Initiative 01 for Consideration	Enhanced set of APIs to support registration updates whilst business is transacting with government agencies without having to return to the federal registration site for update. Must include the surfacing of all information, legal or otherwise at the time of update and in real time, via a central authority to ensure a single, consistent source of truth.		
Initiative 02 for Consideration	New tools to encourage business owners to keep their information up to date		
Initiative 03 for Consideration	Identification and implementation of ‘Roles based model” with the registry services to ensure updates are only completed by authorised people and via the use of secondary identifiers (unique PINS or equivalent).		

Design Question	Consideration	Proposed Strategy	Target Outcomes
ENHANCED REGISTRY SERVICES How we can enhance the services offered and improve the user experience? **Q3.** What services should be provided to allow direct connection from business systems to the registers?	**Our Response** Owners of business systems for small business could fall into the category of software accounting packages or the like. Where the systems are standalone, APIs could be provided to software companies to ensure updated information within the software package owned by the business is able to be provided to government by following a standard model that includes authorisation. Where the solution is cloud based, the use of APIs via the software companies should employ techniques to ensure that no registry information is held/accessible by the software company at any time or under any circumstance.	**Our Response** A. Develop a set of rules for use of API's by 3rd parties that covers privacy, use and non-storage of sensitive registry data B. Ensure updates are only completed by authorised people via the use of secondary identifiers (unique PINS or equivalent). C. Ensure the solution supports and manages authorised people to update business registry information in terms of their identity, role and responsibilities.	**Our Response** 1. Ensure consistent implementation and use. 2. Encourage regular updates to the register as business goes about its business. 3. Consistent and regular digital interactions by business and the introduction of tools to remind business to update their information. 4. Registrations updated, by the right people to the right time and having the right authority.
Initiative 01 for Consideration	Develop a set of rules for use of API's by 3rd parties that covers privacy, use and non-storage of sensitive registry data.		

PTO

Design Question	Consideration	Proposed Strategy	Target Outcomes
ENHANCED REGISTRY SERVICES How we can enhance the services offered and improve the user experience? **Q4.** What interactions with the Registers should be considered to improve the quality of the registry data? **Q5.** What interactions should be considered to ensure the registry data remains up to date? **Q6.** How do you consider registration, annual review and renewal processes could be improved?	**Our Response** Addressed in Q1-Q3 responses above.	**Our Response** Addressed in Q1-Q3 responses above.	**Our Response** Addressed in Q1-Q3 responses above.
Initiative 01 for Consideration	See Q1-Q3 initiatives and responses		

PTO

Design Question	Consideration	Proposed Strategy	Target Outcomes
ENHANCED REGISTRY SERVICES How we can enhance the services offered and improve the user experience? **Q7.** How do you consider search functions within the Registers could be improved?	**Our Response** Currently users maintain multiple usernames, passwords and websites when providing information to the Government. Further, integration and syncing of various data sources and systems across all tiers of government presents privacy and security challenges. All tiers of government must work together to do more to simply the process and experience for business and thereby deliver tangible improvements and benefit. The introduction of new registers must simplify rather than add further levels of complexity for business.	**Our Response** A. Tell Govt once. Continue this initiative by undertaking further analysis of user needs by developing user personas, user goals and develop user scenario maps, wireframes and interaction prototypes for testing. Use data-driven decision making to determine high priority use cases to further develop and implement. B. Use Asymmetric Key cryptography, where the private key never leaves the Director. As an example: - In order to transact with government agencies, users need to provide a signed transaction, proving to the Agency that they are in fact in possession of the private key and thus the director of company X (linked to the public key). The exact process will be hidden from the end user, but essentially, the director would have a set of two encryption keys, one being completely private and the other public, allowing them to share	**Our Response** 1. No data sync issues, as updates are made at a single location and the data is owned by the director. 2. Directors are able to delegate, per transaction or a group of transactions. 3. If user wants to purchase the hardware, the private key never leaves the hardware device and there is a 24-character pass phrase to recover the account in case of lost / stolen hardware. The device can only be accessed after entering a 16-digit code, and runs on its own firmware, so is tamper proof- and only needs to be connected when making a transaction. The software wallet is also highly secure. 4. Two-step verification services can be added to provide further security (i.e. google authenticator) the user will access this on their mobile. Loss of mobile can allow alternate reset mechanisms.

		information with public services. C. Principles underpinning this type of implementation; 1 – User control and consent – Information that identifies the user should only be revealed with that user's consent. 2 – Minimal disclosure for a constrained use – Identity information should only be collected on a "need-to-know" basis and kept on a "need-to-retain" basis. 3 – Justifiable parties – Identity information should only be shared with parties that have a legitimate right to access identity information in a transaction. 4 – Directed identity – Support should be provided for sharing identity information publicly or in a more discreet way. 5 – Design for a pluralism of operators and technology – A solution must enable the inter-working of different identity schemes and credentials. 6 – Human integration – The user experience must be consistent with user needs and expectations so that users are able to understand	5. Solution is highly secure 1) Low requirement of computational power; 2) No requirement of communication between agencies to reach consensus; 3) System continuity independent of the number of available genuine agencies; 6. Encrypted exchange of data to those authorised, and not visible to prying eyes. 7. Support future implementations in IoT tags or sensors, where you will not have to communicate with humans i.e. say tap your RFID sensor and enter biometrics and a passcode to commit to a business transaction.

		the implications of their interactions with the system. 7 – Consistent experience across contexts – Users must be able to expect a consistent experience across different security contexts and technology platforms. D. Delegations based on Cryptography (by example you can generate any number of “aliases” linked to a public key, but for it to be a valid delegation, that transaction or group of transactions will have to be signed using the private key) E. Multi-factor authentication F. Software as well as hardware implementation of Keys (based on AES 256 elliptic curve) G. Future proof though the use of blockchain (a government operated private blockchain). H. Easy flow of data to the people who need it, when they need it	
Initiative 01 for Consideration	Tell Govt once. Continue this initiative by undertaking further analysis of user needs by developing user personas, user goals and develop user scenario maps, wireframes and interaction prototypes for testing. Use data-driven decision making to determine high priority use cases to further develop and implement.		

Initiative 02 for Consideration	Use Asymmetric Key cryptography, where the private key never leaves the Director.
Initiative 03 for Consideration	Delegations based on Cryptography and Multi-factor authentication.
Initiative 04 for Consideration	Future proof though the use of blockchain (a government operated private blockchain).

PTO

Design Question	Consideration	Proposed Strategy	Target Outcomes
FUTURE REGULATORY INFRASTRUCTURE How should we fund the business registers in the future? **Q8.** What types of API users (e.g. registrants, intermediaries, data consumers) could the Charging Framework appropriately apply to? **Q9.** What fee structures should be considered if the Charging Framework was applied? For example, should data users be charged a "per transaction" fee or an "annual subscription fee". **Q10.** What access rules should be placed on API users to facilitate innovative use of registry data?	**Our Response** Our response is aligned to each question below. Government should fund all aspects of registers and operations until they can show value to relevant stakeholders exceeding the cost recovery amount charged. Government should fund all aspects of registers and operations until they can show value to relevant stakeholders exceeding the cost recovery amount charged. Q10 was answered via Q1-Q3 above.	**Our Response** A. Baseline the existing operating model for government, agencies and business. B. Establish measures and forecast benefits for the new operating model C. Implement and measure benefits for all stakeholders and derive value delivered to each stakeholder group	**Our Response** 1. Consider a cost recovery model when and only when stakeholder value is determined.
Initiative 01 for Consideration	Baseline the existing operating model for government, agencies and business.		
Initiative 02 for Consideration	Establish measures and forecast benefits for the new operating model		
Initiative 03 for Consideration	Implement and measure benefits for all stakeholders and derive value delivered to each stakeholder group		

Design Question	Consideration	Proposed Strategy	Target Outcomes
DIRECTOR IDENTIFICATION NUMBERS What is the best way to implement a Director Identification Number? **Q11.** What level of identity verification should be required to obtain a DIN? Is it appropriate to use a digital identity to verify the identity of the company director? If not digital, what other identity verification means should be used and why?	**Our Response** The implementation must be future proof, hack proof and avoid having a single point of failure. The user should be able to open a company online, but then must visit any of the various offices around the country for a once off verification of their account. This may include use of biometric data. Different transactions will require different levels of identity verification depending on the nature of transaction.	**Our Response** A. Use of Asymmetric Key cryptography and/or Blockchain B. The rules of the solution could be codified into smart contracts, which are computer codes that can automatically process data and execute protocols on a blockchain. C. Smart contracts could automatically ensure that government departments are compliant with data protection regulation and that databases are accurate and up to date. D. A blockchain network will ensure the citizen is in charge of their identity instead of multiple government agencies holding (often outdated and conflicting) data about the citizen (director). E. The identity can be verified using a combination of factors, like cryptography, One-Time-Password and Biometrics. It should depend on the complexity of the transaction.	**Our Response** 1. The issue with phoenix is resolved and fraud is reduced. 2. The new model would be highly secure as blockchain is safer than centralised databases. 3. Information stored on the ledger is encrypted at all times. In addition, its distributed nature makes it very difficult to hack, as it would require simultaneously hacking into a majority all within a very short time-before the block progresses, of the devices used by the members on a network. This could reduce the risk of identity fraud.
Initiative 01 for Consideration	Use of Asymmetric Key cryptography and optionally Blockchain		

Design Question	Consideration	Proposed Strategy	Target Outcomes
DIRECTOR IDENTIFICATION NUMBERS What is the best way to implement a Director Identification Number? **Q12.** Ensuring that all directors consent to their role as a company director will be an important part of forming a company and maintaining its registration. What is the most appropriate and efficient manner of gaining a director's consent before issuing a DIN?	**Our Response** This can be very easily achieved when the bigger issue of identity is solved. Asymmetric Key cryptography and use of biometrics will ensure that the person consenting to their role are actually who they claim to be.	**Our Response** A. Asymmetric Key cryptography and optionally Blockchain B. The rules of the solution would be codified into smart contracts, which are computer codes that can automatically process data and execute protocols on a blockchain.	**Our Response** 1. Reduction in fraud. 2. Easy history and analytics to indicate who has engaged in fraudulent behaviour 3. Data matching to weed out the malefactors
Initiative 01 for Consideration	Asymmetric Key cryptography and optionally Blockchain.		
Initiative 02 for Consideration	The rules of the solution would be codified into smart contracts, which are computer codes that can automatically process data and execute protocols on a blockchain.		

Design Question	Consideration	Proposed Strategy	Target Outcomes
DIRECTOR IDENTIFICATION NUMBERS What is the best way to implement a Director Identification Number? **Q13.** Should the law allow authorised agents to apply for a DIN on behalf of their client? If so, how does this fit in the consent framework?	**Our Response** Yes. It is better to not restrict the flexibility of the solution. At the same time, offer the clients to complete the process very easily through the government, making it very easy and intuitive, and quicker. Authorised agents would never have access to private keys. This will naturally lead to clients going to the government directly, instead of via the agent.	**Our Response** A. This can be handled using Asymmetric Key cryptography and optionally Blockchain. B. Include manual step of identity verification and biometrics to reduce fraud. C. The authorised agent would be held accountable if they have knowingly aided and abetted fraud.	**Our Response** 1. Simplified, fraud free solution fit for the future.
Initiative 01 for Consideration	Asymmetric Key cryptography and optionally Blockchain		

Design Question	Consideration	Proposed Strategy	Target Outcomes
DIRECTOR IDENTIFICATION NUMBERS What is the best way to implement a Director Identification Number? **Q14.** What DIN related data should be made publicly and privately available (that is, only available to regulators)? Does the provision of a DIN remove the need to make director and other company officer address data publicly available? What privacy and security concerns are there around the public availability of the DIN?	**Our Response** Our response is aligned to each question below. The online public version of the DIN register should incorporate lessons learned from existing registry deployments and not enable identity theft or misuse. Ideally this would be the appropriate outcome. Refer to Q1-Q3 response. Fraud, institutional and private misuse and institutional data mining that had the potential to undermine the value and potential of the business.	**Our Response** A. Refer to Q1-Q3 response.	**Our Response** 1. Refer to Q1-Q3 response.
Initiative 01 for Consideration	Refer to Q1-Q3 response.		