

Modernizing Digital Identity for National Defence

In the government defence environment, robust and adaptable digital identity solutions are paramount.

This case study details how Intercede, a specialist in credential management systems, and Entrust, the global leader in identity-centric security solutions, partnered with a key technology and infrastructure advisory body within a national Ministry of Defence in the Asia Pacific region to modernize their digital identity infrastructure, enhance security postures, and ensure long-term operational resilience.

THE CHALLENGE

The Customer faced a multifaceted challenge in their ongoing programme to refresh and update their technology infrastructure. Their existing Public Key Infrastructure (PKI) and Credential Management System (CMS), along with end-user device components, were outdated and nearing the end of their operational lifespans. Key objectives for this refresh included:

ENHANCED SECURITY: There was a pressing need to support more sophisticated security mechanisms to counter evolving threats.

STANDARDS COMPLIANCE: A fundamental requirement was full support for the FIPS 201 Personal Identity Verification (PIV) standard.

VENDOR INDEPENDENCE & FLEXIBILITY: The Customer sought to reduce vendor lock-in and introduce greater flexibility for future technology decisions, ensuring adaptability to emerging standards and solutions.

USER EXPERIENCE OPTIMIZATION: The organization aimed to integrate and manage biometrics to simplify the user experience without compromising stringent security protocols.

TRANSITIONING PKI: A critical PKI component had reached its end-of-life, posing significant security and support risks.

FAST-TRACK DEPLOYMENT: The Customer required design, build and implementation of the solution within a challenging timeframe to meet their internal governance.

THE SOLUTION

Intercede undertook a thorough requirement gathering session. This involved close collaboration with other vendors contributing to the solution stack, ensuring seamless integration and a holistic approach. The implemented solution encompassed:

SCALABLE ARCHITECTURE: Leveraging Intercede's MyID CMS, a solution architecture was deployed to support multiple air-gapped environments, managing tens of thousands of end-user devices. This architecture was designed to initially support Idemia smartcards while maintaining future scalability for a wide array of future end-user devices, including mobile platforms, USB tokens, and virtual smartcards.

PKI INTEGRATION: Established seamless integration with a new PKI solution provided by Entrust, ensuring a robust and modernized cryptographic foundation.

CUSTOM APPLET SUPPORT: The solution facilitated support for custom applets on smartcards, enabling tailored functionalities specific to the Customer's operational needs.

ENHANCED END-USER DEVICE SECURITY: Biometric Match-on-Card authentication was introduced to significantly enhance the user experience and security of end-user devices, providing a strong, multifactor authentication mechanism.

SECURE KEY STORAGE: MyID SecureVault, delivered the customer a new CA independent Key Storage solution, providing secure and managed access, generation and recovery of highly sensitive cryptographic key material. This was a critical component to maintain data integrity and confidentiality in line with the organisations strict security policies.

"Our engagement with the Customer was a testament to deep collaboration. By meticulously understanding their intricate requirements and working together with their ecosystem of technology partners, we were able to create a comprehensive digital identity framework. The integration of MyID CMS and MyID SecureVault ensures not just immediate operational resilience, but also provides the foundational agility for their future security endeavours."

Siobhan Morey-Millington, Sales Director, Intercede

Lawerence Tan, Entrust Technical Sales Director said: "Collaborating on this project allowed us to deliver a modern PKI solution that seamlessly integrated with the broader digital identity framework. The synergy between our PKI and Intercede's MyID CMS was crucial in meeting the Customer 's stringent security and compliance objectives, especially around FIPS 201 PIV. It's a prime example of how integrated, standards-compliant solutions elevate an organization's security posture."

THE RESULTS

The organisation is currently in the process of rolling out the solution across its separate environments. This phased deployment is already enabling the identification of additional functionalities, such as secure, separate biometric storage, which will further enhance the organization's flexibility and overall security capabilities.

The complete solution and end-user rollout are targeted for completion by December 2026, with a strategic intention for the system to remain operational for at least eight years as an integral part of the overall contract. This project establishes a resilient, adaptable, and highly secure digital identity infrastructure, positioning the organisation to meet evolving defence sector demands effectively.

CONTACT US TO FIND OUT MORE

Contact us today and discover what MyID CMS and MyID SecureVault can do for your organisation:

info@intercede.com

+44 (0)1455 558 111

+1 888 646 6943