ARTHUR VAN DER MERWE

- Sydney, Australia
- 0447832066
- arthurvdmerwe@me.com
- arthurvandermerwe.com

Memberships

International Association for Cryptologic Research

Institute of Electrical and Electronics Engineers

BCS - Chartered IT Professional

Certifications

Java Certified Professional Developer

Microsoft Certified Solutions Developer

SafeNet Certified KeySecure Engineer

SafeNet Certified Pheft Engineer

Thales Certified Payshield Engineer

SAFe Agilist (SA) certified

ITIL Foundation Certification

Published articles

- The Refund vulnerability of AS2805 and EFTPOS
- Data Security – RSA
- DUKPT Explained with examples
- EFTPOS Initialisation using RSA Cryptography
- ATM Pin encryption using 3DES
- Implementing AS2805 Part 6 Host to Host Encryption using a Thales 9000 and Python
- Typical Cryptography in AS2805 Explained
- Thales 9000 with AS2805 Interchange & RSA EFTPOS Commands.
- Thales Key Exchange Examples and Troubleshooting
- Testing DUKPT
- Parsing AS2505/8583 Messages
- Dynamic Key Exchange Models
- Doing PIN Translation with DUKPT

Summary

I bring a wealth of experience, having worked in various areas such as software engineering, agile management methodologies, compliance, cryptography, and cybersecurity management. I take pride in learning from every experience and fully applying my knowledge and experience in all areas to push boundaries. While I am known for my technical prowess, I can step back and consider a strategic view of technologies and present them to C-level executives.

My passion for learning drives me to constantly explore new technologies and consider how they may disrupt the current status quo. This passion for research is evident in my blog and my work with UNE. I have a solid foundation in security and technology, which has allowed me to make a substantial impact on improving security, business, and technology systems. I have demonstrated business knowledge and a pragmatic approach to resolving industry and security issues.

Having extensive experience in technical cyber, theoretical cryptography, governance and risk management, people management, influencing and leadership, my skills are well rounded and deep.

- Credit vs Debit
- AS2805 Standards for EFT
- Trace your ATM Transactions

Publications

BSc Hons - AS2805 Processing Systems within Distributed Networks

MSc - Searchable Encryption schemes from Identity based encryption schemes and bi-linear maps.

<u>Journal Publications</u>

Security in banking - a review of AS805 and TR-31

Keyed block s-boxes from Sponges.

The design of the Ubox cipher.

Education

PhD - Doctor of Philosophy
University of New England, Armidale, Australia
Cryptography

MSc - Master of Science Degree (Distinction)
University of Hertfordshire, St Albans, United Kingdom
Computer Science & Cybersecurity

BSc (Hons) - Bachelor of Science, Honours (Distinction)
University of Hertfordshire, St Albans, United Kingdom
Computer Science & Cybersecurity

Postgraduate Certificate
Stanford University, Serra Mall, Stanford, CA
Computer Science & Cybersecurity

Work History

<table>
<tr><td>2022 - Current</td><td>Senior Specialist - Cyber Supervisory and Operational Resilience.
Australian Securities and Intvestment Commission (ASIC)</td></tr>
</table>

2022 - Current

Senior Specialist - Cyber Supervisory and Operational Resilience.

Australian Securities and Intvestment Commission (ASIC)

2018 - 2022

Security and Industry Compliance Manager - Security, Assessments, Standards and Compliance

Australian Payments Network (APCA)

As a Governance, Risk, and Projects expert, I have extensive experience in Payment Acceptance Governance. I led the work aligning payment acceptance devices to the PCI SSC Standards. Additionally, I designed and implemented risk models to evaluate non-standard payment technology for Compliance Risk Models.

I also actively participated in the design of secure APIs for Consumer Data Right - Open Banking. Furthermore, I designed and facilitated accreditation frameworks for digital identity for Trust ID - Digital Identity. I also created and implemented enforcement models for Compliance Design/ Implementation compliance regimes.

Stakeholder Management is also an area of my expertise, where I manage various (third-party and internal) stakeholders, from technical experts to C-level executives. Moreover, I actively advise industry committees on emerging issues in payments and security for Industry Advisory Committees - technical management and board.

I have extensive experience managing and running compliance programs for the annual acquirer and issuer audits for card payment systems, ensuring integrity across submissions and non-compliance exemptions. I also assess payment devices' security capability and vulnerabilities and approve devices and payment software that can be used in Australia. Furthermore, I consider HSM evaluation reports and API functions for use in Australia, ensuring vendors meet Australian and international cryptography standards.

I advised members (Australian Banks, Acquirers, and Vendors) on security, compliance, and emerging industry developments. I also promote innovative (secure) solutions to enter the Australian Payments market.

In Information Security, I defined and managed industry Security and Standards Roadmaps, ensuring industry security posture. I am also an author and advisor for industry security standards development. Moreover, I tend industry projects to migrate cryptography mechanisms, ensuring industry-wide and international interoperability.

I participated in industry groups, such as FIDO, Digital Identity, and International Standards, ensuring frameworks and security are aligned with global best practices for authentication, cryptography, and privacy. Additionally, I advise industry security committees on security best practices and current vulnerabilities. I also continually review industry security guidance and rules, aligning rules with industry best practices.

Lastly, I present at Universities and Conferences on security-related topics, like AWS hacking, security awareness, PAM, and digital identity. I sit on Industry, National, and International committees, defining security standards and evaluation requirements to secure payments and data. Industry PCI and EMV committees include Payment Card Industry Security Standards Council (PCI-SSC) Technical Advisory Board, Payment Card Industry (PCI) PIN Transaction Security Working Group, Payment Card Industry (PCI)-Software Security Standards Working Group, Payment Card Industry (PCI) Mobile Working Group (SPoC & CPoC), and EMV co - Tokenisation.

I was also a member of National Standards Committees, such as IT-005 - Financial Transaction Systems - Standards Australia, IT-004 Blockchain - Standards Australia, IT-005-4 Authentication and Security - Standards Australia, and IT-005 - Standards Australia, AS2805 Standards Drafting Lead, IT-043 - Artificial Intelligence - Standards Australia, and IT-12 -

Information Systems, Security and Identification Technology. Additionally, I am a member of International Standards Committees, such as ISO/TC 68/SC 2/WG 13 Security in retail banking, Member, and ISO/TC 68/SC 2/WG 11 Encryption algorithms used in banking, and Member applications.

In the Australian Payment Industry Committees, I was part of the AusPayNet HSM/SCM Working Group Drafting Lead and AusPayNet Management member: Technical Sub-Security Committee and Technical Security Committee.

2017 - 2018   Principal Information Security, Consultant - Cryptography
Westpac Group

At Westpac Group, I managed BAU operations and various projects related to Core Technologies, such as Python, C#, and Web API. I also oversee the use of Gemalto and Thales nShield HSMs, including Gemalto Key Secure, Gemalto ProtectV Manager, Gemalto Protect File, Gemalto Protect App, and Gemalto Luna HSM. Additionally, I lead the BAU operation for Hybrid Cloud Encryption, develop client onboarding procedures, and maintain transparent disk encryption operations and practices for over 3000 servers.

As part of my responsibilities, I manage and maintain a 24/7 support roster and on-call operations and act as the support lead for escalating platform issues and resolutions. I also build and maintain HSM infrastructure, including Thales nShield (x8), Safenet PHEFT (x16), and Safenet Luna (x8), and oversee key operations and procedures for Public Key Infrastructure and Payments (Base 24) platforms.

To ensure compliance with PCI PIN Audit operational policies and procedures, I am responsible for maintaining and managing the Gemalto KeySecure platform, including designing and developing client onboarding procedures for key management, folder and file-based encryption procedures, and optimizing BAU and project operations with Python and Perl automation.

2012 - 2017   Senior Manager - Information Security, IT & Software Development
Cashpoint Payment Solutions & SwitchLink Financial Processing

As a Senior Manager for Information Security, IT, and Software Development at Cashpoint Payment Solutions & SwitchLink Financial Processing, I oversaw various core technologies and services such as software development services using C# and Python, PKI Infrastructure, Kaspersky Endpoint, Custom Vault PAM, AlienVault SOC, Fortinet IDS and IPS, and Thales General-purpose and Payments HSM fleet. I also led terminal software development using ASP.Net and Winforms, web software development using MVC4, MVC5, and Asp.net Core, API software development using Web API and Secure Sockets, third-party software development using Entity Framework, AngularJS, JavaScript, HTML5, and CSS3. Additionally, I provided source control services using Git and database services using SQL Server, MySQL, and Oracle. I had experience working with Azure and AWS cloud environments, Continuous Integration (CI) with TFS, Test-Driven Development (TDD) procedures, and Thales Payshield 9000 HSMs. I built and managed custom-built Payments Platforms.

My role involved promoting and driving a strong risk culture that ensures risk/reward considerations are integral to business decision-making and supports the delivery of business objectives. I reviewed new business opportunities to ensure that key operational risks were identified and managed. I developed and maintained a product development roadmap, led continuous improvement initiatives, and researched payment trends such as tokenisation. I maintained PA-DSS policies within the Payment Processing Platforms. I implemented and managed regulatory policies mandated by VISA, MasterCard, APCA, and APRA. I developed business cases for the inclusion of features within switching platforms, maintained ATM and EFTPOS network processing and monitoring systems, and managed and maintained Customer Management Systems.

I elicited requirements from the business to maintain the product plan and future roadmap, maintained prioritisation of features, and led requirements gathering. I led workshops for business and process improvement initiatives, documented requirements using formal methods, and managed and maintained IT infrastructure. I developed and implemented processes and procedures for managing the infrastructure, PCI DSS Policies and Procedures, Operational Policies and Procedures, and VISA/Mastercard Pin Compliance policies. I managed a strong culture to automate compliance and regulatory requirements.

I managed the software development team, maintained a backlog of development items, and reprioritised as required. I developed statistics on the maintainability of systems, produced metrics of development team performance and progression of projects, and drove technical training within the unit. I evaluated new technologies and market research, implemented and maintained Change Management Processes and Procedures, and managed and maintained Cryptographic Infrastructure such as HSM Management, Key custodian and generation and maintenance policies and procedures, and PKI Infrastructure. I also managed cloud and remote encryption capability and device security.

My notable achievements include starting with a clean slate of no existing software and architecting a new codebase implemented with .NET and C#. I championed technical innovation in the User Interface Design to facilitate production tests and complement new measurement techniques, led the team to develop a new product platform and family of multi-channel world-class transaction processing and monitoring systems, introduced Agile into a willing environment, and stabilised the custom integration process by creating a QA department and testing procedures. I designed and documented multiple APIs to ease the integration process for clients, spearheaded the implementation of the company's first-ever disaster recovery system to ensure minimal productivity loss, developed and implemented a new customised product to process transactions for large deployers, managed a portfolio of programs/projects, maintained ISO and VAR relationships as well as vendor selection, performed audits at Data Center, redesigned and architected several existing components in the system, lead the design and architecture activities for all new development work, defined and enforced development, build and release processes, and evaluated server software and helped in the decision-making process for retooling the application to consolidate technologies.

2012 - 2012   Software Development Manager
Digital Visual Technologies - Direct Axis

2006 - 2012   Senior Financial Systems Manager
Spark ATM Systems

2006 - 2008   Principal Solutions Architect - Application Solutions
Dimension Data - Africa & Asia

2005 - 2006   Integration Analyst Developer
Woolworths Financial Services - Africa

2001 - 2005   Software Developer
Ferreira Technologies