



ARTHUR VAN DER MERWE

Never Stop Learning

📍 Sydney, Australia

☎ 0447832066

✉ arthurvdmerwe@me.com

🌐 arthurvandermerwe.com

Memberships

International Association for Cryptologic Research

Institute of Electrical and Electronics Engineers

BCS - Chartered IT Professional

Australian Information Security Association - Member.

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

Summary

I have a wealth of experience in various areas, such as software development, agile management methodologies, compliance, cybersecurity management, I pride myself to learn from every experience, and apply my knowledge/experience fully in all areas to push boundaries. Colleges often see me as very technical in nature, with the ability to step back and consider a strategic view of technologies.

I have a passion for learning where I constantly exploring new technologies and considering how they disrupt the current status quo. My passion for research is clearly demonstrated in my personal blog and my work with UNE. I have been well versed in the security and technology field of Australia and hope to continue my momentum to make a substantial impact on the improvement of business and technology systems. I intend to do this by demonstrating business knowledge and a pragmatic approach to resolving industry issues.

My personal projects include Research with the University of New England, where I evaluate mathematical models or tamper-proof and authenticated encryption schemes. Other projects include contributing to technical blogs and publishing papers on cryptography as well as a vast collection of code on GitHub and coding in my spare time.

- Dynamic Key Exchange Models
- Doing PIN Translation with DUKPT
- Credit vs Debit
- AS2805 Standards for EFT
- Trace your ATM Transactions

Published research papers

University of Hertfordshire - AS2805 Processing Systems within Distributed Networks

University of Hertfordshire - Searchable Encryption schemes from Identity based encryption schemes and bi-linear maps.

Security in banking

Current Research Areas

Payment processing implementations using contemporary technologies.

Low cost Networking models for payment systems communications.

Signature and Certificate based key injection models

Security in Banking

Skills

People Management



Solution Architecture



Service management



Cryptography



AS2805



Education

PhD - Doctor of Philosophy

University of New England, Armidale, Australia

Part-Time Research Candidate

Computer Science & Cybersecurity

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

2018 - Present

Manager - Information Security and Industry Compliance Australian Payments Network (APCA)

Industry Compliance

Proactively manage and run compliance programs for the annual acquirer and issuer audits for card payment systems, ensuring integrity across submissions, and non-compliance exemptions.

Assess and manage the assessment of payment devices in their security capability and vulnerabilities, and approve devices and payment software which can be used in Australia.

Assess HSM evaluation reports and function sets for use in Australia ensuring vendors meet Australian and international cryptography standards.

Advise members (Australian Banks, Acquirers, and Vendors) on security, compliance, and industry developments.

Promote innovative solutions to enter the Australian Payments market.

Information Security

Define and manage industry Security and Standards Roadmaps ensuring industry security posture.

Manage industry projects to migrate cryptography mechanisms ensuring industry-wide and international interoperability.

Participate in industry groups, such as FIDO, Digital Identity, International Standards, ensuring frameworks and security are aligned with global best practices for authentication, cryptography, and privacy.

Advise industry security committees on security best practices and current vulnerabilities. Continually review industry security guidance and rules, aligning rules to industry best practices.

Present at Universities and Conferences on security-related topics, like AWS hacking, security awareness, PAM and digital identity.

Working Groups, Committees and Memberships

Sit on Industry, National and International committees, defining security standards and evaluation requirements to secure payments and data. These 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)
- EMV co - Tokenisation
- AS2805 - Standards Australia - IT-005 Financial Transaction Systems
- Blockchain - Standards Australia - IT-005-4 Authentication and Security
- ISO/TC 68/SC 2/WG 13 Security in retail banking, Member
- ISO/TC 68/SC 2/WG 11 Encryption algorithms used in banking, Member applications
- AusPayNet HSM/SCM Working Group Drafting Lead
- AusPayNet Management member: Technical Sub-Security Committee
- AusPayNet Management member: Technical Security Committee
- Standards Australia. IT-005, AS2805 Standards Drafting Lead

2017 - 2018

Principal Information Security, Consultant - Cryptography Westpac Group

• Compliance

- Run and manage AusPayNet Compliance for Payments HSMs across the Westpac Group

• Core Technologies

- Run BAU operations and various projects with the group technology ensuring operational capacity and service excellence.
 - Python / C# / Web API
 - Gemalto Key Secure
 - Gemalto ProtectV Manager

- Gemalto Protect File
- Gemalto Protect App
- Thales nShield HSM
- Gemalto Luna HSM
- Gemalto PHEFT Payments HSM
- **Lead BAU operation for Hybrid Cloud Encryption**
 - Develop client on-boarding procedures
 - Maintain transparent disk encryption BAU operations and procedures for 3000 + servers.
 - manage and maintain 24/7 support roster and on-call operations
 - Support lead for escalation of platform issues and resolutions.
- **Build and maintain HSM infrastructure**
 - Thales nShield (x8), Safenet PHEFT (x16), Safenet Luna (x8) build and maintenance.
 - Key operations and procedures for Public Key Infrastructure and Payments (Base 24) platforms
 - PCI PIN Audit operational policies and procedures.
- **Key Management Infrastructure**
 - Maintain and manage Gemalto KeySecure platform- build and support
 - Design/Develop client on-boarding procedures for key management
 - Design/Develop Folder and file-based encryption procedures
 - Design/Develop 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

- **Core Technologies and Services**
 - C#, Python - software development services
 - PKI Infrastructure
 - Endpoint - Kaspersky
 - PAM - Custom Vault
 - SOC, SIEM - AlienVault
 - IDS and IPS - Fortinet
 - General-purpose and Payments HSM fleet. (Thales)
 - ASP.Net, Winforms - terminal software development.
 - MVC4 , MVC5, Asp.net Core - web software development.
 - Web API, Secure Sockets - API software development.
 - Entity Framework and other third party software development.
 - AngularJS, JavaScript, HTML5, CSS3
 - Source Control, Git - source control services
 - SQL Server, MySQL, Oracle - database services.
 - Azure and AWS cloud environments.
 - Continuous Integration (CI) with TFS
 - Test-Driven Development (TDD) procedures
 - Thales Payshield 9000 HSMs
- **Build and Manage custom-built Payments Platforms**
 - Promote and drive a strong risk culture that ensures that risk/reward considerations are integral to business decisions making and support the delivery of business objectives
 - Review new business opportunities ensuring that key operational risks are identified and managed
 - Develop and maintain a roadmap of product development
 - Lead continuous improvement initiatives
 - Maintain and Research current payments trends (i.e.tokenization)
 - Maintain PA-DSS policies within the Payment Processing Platforms.
 - Implement and Manage Regulatory policies and mandated by VISA, MasterCard , APCA and APRA.
 - Develop business cases for the inclusion of features within switching platforms.
 - Maintain ATM and EFTPOS network processing and monitoring systems.
- **Manage and Maintain Customer Management Systems**
 - Elicit requirements from business to maintain product plan and

future roadmap.

- Maintain prioritization of features and lead requirements gathering.
- Lead workshops for business and process improvement initiatives.
- Document Requirements using formal methods
- **Manage and Maintain IT Infrastructure**
 - Develop and implement processes and procedures for Managing the Infrastructure
 - PCI DSS Policies and Procedures
 - Operational Policies and Procedures
 - VISA / Mastercard Pin Compliance policies
 - Maintain a strong culture to automate compliance and regulatory requirements.
- **Manage Software Development Team**
 - Maintain backlog of development items and reprioritize as required.
 - Develop statistics on the maintainability of systems.
 - Produce metrics of development team performance and progression of projects.
 - Drive technical training within the unit.
 - Evaluate new technologies and market research.
 - Implement and maintain Change Management Processes and Procedures.
- **Manage and Maintain Cryptographic Infrastructure**
 - HSM Management and development of policies and procedures
 - Key custodian & generation & maintenance policies and procedures.
 - Manage PKI Infrastructure
 - Manage Cloud and remote encryption capability.
 - Manage device security

Several of my notable achievements are listed below:

- Starting with a clean slate of no existing software, Architected a new codebase implemented with .NET and C#.
- Championed technical innovation in the User Interface Design to facilitate production test and compliment new measurement techniques
- Led 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
- Stabilized custom integration process by creating a QA department and testing procedures.
- Created and documented multiple API's to ease the integration process for clients.
- Spear-Headed the implementation of the company's first-ever disaster recovery system to ensure minimal productivity loss.
- Developed and implemented new customized product to process transactions for large deployers.
- Managed 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
- 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

Core Technologies

- C# , Python, Mendix
- ASP.Net
- MVC4
- Web API
- Entity Framework
- AngularJS, JavaScript, HTML5, CSS3
- Source Control, Git
- SQL Server, MySQL, Oracle

- Azure and AWS
- Continuous Integration (CI) with TFS
- Test Driven Development (TDD)
- Continued PCI Compliance Reporting
- Model business processes using contemporary tools and methods
- Evaluate risk and decision modelling platforms
- Review developer code, and produce metrics for maintainability.
- Develop and Maintain business processes for development team.

2006 - 2012 Senior Financial Systems Manager

Spark ATM Systems

- **Core Technologies**
 - C# , Python, Delphi
 - AngularJS, JavaScript, HTML5, CSS3
 - Source Control, Git
 - SQL Server, MySQL, Oracle
 - Azure and AWS
 - Continuous Integration (CI) with TFS
 - Test Driven Development (TDD)
- Architect and Develop Payments Processing Platforms
- Implement EMV processing with Postbridge
- Maintain and develop policies and procedures
- Maintain and Develop PCI and PA DSS Policies and procedures
- Maintain a culture to ensure continued compliance.

2006 - 2008 Principal Solutions Architect - Application Solutions

Dimension Data - Africa & Asia

- **Core Technologies**
 - C# ,VB.net
 - ASP.Net
 - MVC, Webforms, Winforms
 - Web Services
 - Entity Framework
 - AngularJS, JavaScript, HTML5, CSS3
 - Source Control, Git
 - SQL Server, MySQL, Oracle
 - Azure and AWS
 - Continuous Integration (CI) with TFS
 - Test Driven Development (TDD)

Consulting for S1 Postillion

- Postbridge and Real Time Framework enhancements
- Source and Sink Node Templating
- ISO adapter enhancements for spd and AS messaging

Consulting for Vodafone

- Dynamic call routing systems with Genesys and Avaya
- Implemented and Distributed telephony routing systems.

Other Activities:

- Developer Architecture and OO Training
- Billing systems consulting
- Development Management

2005 - 2006 Integration Analyst Developer

Woolworths Financial Services - Africa

2001 - 2005 Software Developer

Ferreira Technologies

Technologies I am Comfortable with

Programming Languages: C#, Java, C, C++, Python

Services: PKI, PAM, HSMs, Endpoint, Cloud, SOC, SIEM.

Web Frameworks: MVC, ASP.net, Web API, SignalR, Quartz, OpenID, SAML

Front End Frameworks: Bootstrap, NodeJs, Angular, MVC

Server Frameworks: Kafka, RabbitMQ, ActiveMQ, ZeroMQ, SQL, MySQL, Oracle

Networking: Fortinet, Cisco, F5, Dell, BGP

Encryption Hardware: Thales Payshield 9000, Thales nShield, Safenet Luna, Safenet PHEFT

Hobbies

- Research: Security in Banking, AS2805 and TR-31 mathematical models.
- Outdoor: Fishing
- Outdoor: Motorbike racing
- Outdoor: Target shooting (professional)