# Securing a real-time field area network using smart cards

by

**Gerhard Petrus Hancke**

Submitted as partial fulfillment of the requirements for the degree
Master of Engineering (Computer Engineering)
in the
Faculty of Engineering
UNIVERSITY OF PRETORIA

August 2003

# Summary

Field area networks are rapidly expanding to include a wide range of applications. Intelligent nodes on the network will be installed in a small to medium geographical area to monitor and control processes. Such nodes are generally connected to a centralized gateway used by a service provider to monitor and control various applications. The growth in popularity of ubiquitous computing requires the use of embedded network processors in everyday objects. Even though the idea of interaction between the digital devices around us could bring a great deal of convenience it also introduces great risks. Therefore such applications would not only require measurement, control and communication functionality but also a high level of security.

Smart cards offer a simple, inexpensive method of incorporating a cryptographic processor into an embedded system that will allow for the implementation of security services. A field area network has resource limitations that influence security service implementation, such as low bandwidth, limited processing power, limited storage capacity and limited communication protocols.

This dissertation discusses the implementation of a security policy for embedded field area networks used in distributed real-time applications, using smart card technology. The primary objective is to formulate a policy that can be implemented to secure a field area network. The secondary objective is to determine whether this policy can be implemented using mechanisms provided by smart card technology, while maintaining reasonable system performance. It states the approach taken to finding a viable solution to the problem defined above. A comprehensive literature study provides background on relevant technology and possible solutions. In a system overview the system's boundaries and functional requirements are defined. The implementation section outlines possible solutions and descibes how these can be implemented. Evaluation, verification and quantification of the performance of the proposed system are performed according to the experimental procedures described. The results obtained are documented and discussed. In the conclusion the proposed solution and the findings from the results are placed in context. Future topics of research in this field are suggested.

**Keywords**: cryptography, field area networks, smart cards, information security

# List of Abbreviations

**AES** - Advanced Encryption Standard
**API** - Application Programmers Interface
**BMA** - British Medical Association
**CA** - Certification Authority
**CLEF** - Commercial Licensed Evaluation Facilities
**COBIT** - Control Objectives for Information and Related Technologies
**COS** - Card Operating Systems
**CTPEC** - Canadian Products Evaluation Criteria
**CRAMM** - UK Government's Risk Analysis and Management Method
**DES** - Data Encryption Standard
**DF** - Dedicated Files
**DSA** - Data Signature Algorithm
**DSS** - Data Signature Standard
**EEPROM** - Electrically Erasable Programmable Memory
**EF** - Elementary Files
**FAN** - Field Area Network
**FIPS** - Federal Information Processing Standards Publications
**GMITS** - Guidelines for the management of IT security
**IETF** - Internet Engineering Task Force
**ITSEC** - Information Technology Security Evaluation Criteria
**ITU-T** - International Telecommunication Union Standardization Sector
**IVV** - Independent Verification and Validation
**MAC** - Message Authentication Code
**MASC** - Multi-Application Smart Card
**MD** - Message Digest
**MOAS** - Multi-Application Operating Systems
**OP** - Open Platform
**OSI** - Open System Interconnection
**PDA** - Personal Digital Assistant
**PIN** - Personal Identification Number
**PKI** - Public Key Infrastructure
**QoS** - Quality of Service
**RAM** - Random Access Memory

**RFC** - Request for Comments
**ROM** - Read Only Memory
**RSA** - Rivest Shamir Adelman
**SHA** - Secure Hash Standard
**SP** - Service Provider
**TCP/IP** - Transfer Control Protocol/Internet Protocol
**TOE** - Target of Evaluation
**VM** - Virtual Machine
**VOP** - VISA Open Platform

# Contents