

# 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

Keywords: smart cards, real-time, field area network, security, authentication, authorization, access control, cryptography, smart card, real-time, field area network, security, authentication, authorization, access control, cryptography, smart card

## 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 describes 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

<b>1</b>	<b>Research Overview</b>	<b>1</b>
1.1	Introduction . . . . .	2
1.2	Problem Statement . . . . .	4
1.3	Scope . . . . .	4
1.4	Research Context . . . . .	5
1.5	Research Objectives . . . . .	5
1.6	Research Approach . . . . .	7
1.6.1	Research Method . . . . .	8
1.7	Document Overview . . . . .	9
<b>2</b>	<b>Literature Study</b>	<b>11</b>
2.1	Overview and Related Work . . . . .	12
2.2	Information Security . . . . .	13
2.2.1	Security Mechanisms . . . . .	15
2.2.2	Security Threats . . . . .	16
2.2.3	Security Services . . . . .	18
2.2.4	Security Assurance . . . . .	30
2.2.5	Key Management . . . . .	32
2.3	Distributed Field Area Networks . . . . .	33
2.3.1	Security in Embedded Systems . . . . .	36
2.4	Smart Card Technology . . . . .	37
2.4.1	Smart Card Architecture . . . . .	37
2.4.2	Smart Card Operating Systems . . . . .	45
2.4.3	Why Use Smart Cards? . . . . .	54
<b>3</b>	<b>System Overview</b>	<b>56</b>
3.1	System Definition . . . . .	57

3.1.1	System Architecture . . . . .	58
3.1.2	Assumptions . . . . .	58
3.2	Risk Analysis . . . . .	60
3.2.1	Identification of Assets . . . . .	60
3.2.2	System Requirements . . . . .	61
3.2.3	Vulnerabilities and Threats . . . . .	62
<b>4</b>	<b>System Specifications</b>	<b>65</b>
4.1	Security Policy Overview . . . . .	66
4.2	System Components . . . . .	66
4.2.1	Node . . . . .	67
4.2.2	Private Network . . . . .	69
4.2.3	Public Network . . . . .	70
4.2.4	Gateway . . . . .	71
4.2.5	Owner . . . . .	72
<b>5</b>	<b>Implementation</b>	<b>74</b>
5.1	Security Services . . . . .	75
5.1.1	Availability . . . . .	75
5.1.2	Authentication . . . . .	75
5.1.3	Access Control . . . . .	76
5.1.4	Integrity and Non-repudiation . . . . .	77
5.1.5	Confidentiality . . . . .	78
5.1.6	Key Management . . . . .	78
5.2	System Components . . . . .	80
5.2.1	Node . . . . .	80
5.2.2	Private Network . . . . .	82
5.2.3	Public Network . . . . .	83
5.2.4	Gateway . . . . .	83
5.2.5	Owner . . . . .	85
5.3	Security Policy Overview . . . . .	86
5.3.1	Node Registration . . . . .	87
5.3.2	Owner $\Rightarrow$ Node . . . . .	90
5.3.3	Node $\Rightarrow$ Owner . . . . .	93
5.3.4	Node $\Leftrightarrow$ Node: Trusted Gateway . . . . .	97

5.3.5	Node $\Leftrightarrow$ Node: Untrusted Gateway . . . . .	100
5.3.6	Node $\Leftrightarrow$ Node: Direct . . . . .	103
5.3.7	Key Management . . . . .	104
5.3.8	Additional Considerations . . . . .	104
5.4	Mechanism implementation . . . . .	104
5.4.1	Confidentiality . . . . .	107
5.4.2	Digital Signature: PKI . . . . .	107
5.4.3	MAC: Symmetric encryption . . . . .	108
5.4.4	Authentication: PKI . . . . .	108
5.4.5	Authentication: Symmetric . . . . .	109
5.4.6	Messages . . . . .	109
<b>6</b>	<b>System Evaluation</b> . . . . .	<b>110</b>
6.1	Security Assurance . . . . .	111
6.2	Performance of Security Mechanisms . . . . .	112
6.3	Test System . . . . .	113
<b>7</b>	<b>Results</b> . . . . .	<b>116</b>
7.1	Security Assurance . . . . .	117
7.2	Performance of Security Mechanisms . . . . .	120
7.2.1	Confidentiality . . . . .	121
7.2.2	Digital Signatures . . . . .	121
7.2.3	Authentication: PKI . . . . .	121
7.2.4	Authentication: Symmetric . . . . .	125
7.2.5	Messages . . . . .	126
<b>8</b>	<b>Conclusion</b> . . . . .	<b>127</b>
8.1	Summary of the Work . . . . .	128
8.2	Summary of the Results . . . . .	128
8.2.1	Effectiveness of Security Policies . . . . .	128
8.2.2	Comparison of Security Policies . . . . .	129
8.3	Conclusions . . . . .	129
8.4	Suggestions for Future Work . . . . .	130
<b>9</b>	<b>References</b> . . . . .	<b>131</b>