شبكة المعلومـــــات الجامعية

التوثيق الالكتروني والميكروفيلم

شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الالكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأفلام قد اعدت دون آية تغيرات

يجب أن

تحفظ هذه الأفلام بعيداً عن الغبار

في درجة حرارة من 15 – 20 مئوية ورطوبة نسبية من 20-40 %

To be kept away from dust in dry cool place of
15 – 25c and relative humidity 20-40 %

Ain Shams University Information Network

جامعة عين شمس

شبكة المعلومات الجامعية

@ ASUNET

بعض الـوثـــائق

الأصـلية تـالفـــة

SOLVING THE E-SIGNATURE NON-REPUDIATION PROBLEM

By

Hani Samuel Kirollos

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

Faculty of Engineering, Cairo University
Giza, Egypt
2007

SOLVING THE E-SIGNATURE NON-REPUDIATION PROBLEM

By

Hani Samuel Kirollos

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

Supervised by

Prof. Dr. **Ahmed Mahmoud Darwish**
Minister of State for Administrative Development

Faculty of Engineering, Cairo University
Giza, Egypt
2007

SOLVING THE E-SIGNATURE NON-REPUDIATION PROBLEM

By

Hani Samuel Kirollos

B.Sc. in Computer Engineering – Cairo University

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

Approved by the Examining Committee:

A.M. Darwish

Prof. Dr. **Ahmed Mahmoud Darwish**, Minister of State for Administrative Development, Thesis Advisor

Prof. Dr. **Mohammed Saad El-Sherif**, Member

Prof. Dr. **Aly Aly Fahmy**, Member

A. Fahmy

Faculty of Engineering, Cairo University
Giza, Egypt
2006

ACKNOWLEDGMENTS

First, I would like to thank God Almighty for his great grace that He gave me to do this work. I clearly see that his blessings to me are behind all this work.

Next, I would like to thank Prof. Dr. Ahmed Darwish, Minister of State for Administrative Development, for his great kindness to diligently supervise this thesis and for teaching me for more than ten years which showed his very sweet and loving excellent character.

I would like to thank very much Prof. Dr. Nevin Drawish for the great encouragement and the advices that she gave me.

I would also like to thank Prof. Dr. Mohammed El-Sherif for his great efforts and advices.

Likewise I would like to thank my parents, Dr. Samuel Kirollos Girgis and Dr. Elaine Younan Hanna for their continuous encouragement to me.

ABSTRACT

Signature Creation Devices such as smart cards or tokens that comply with the European E-Signature Directive are vulnerable to Trojan Horses attacks through which an attacker can fraudulently create digital signatures utilizing the user's signature creation device when it is used on an infected computer. The current antivirus technologies cannot fully protect from polymorphic Trojan Horses that change their shapes frequently with time. Hence non-repudiation cannot be satisfied because the signor cannot ultimately protect himself.

Existing solutions in the prior art have various limitations, including device size, suitability for un-trusted computers such as Internet café computers and scalability with regards to the size of the data that can be reviewed and signed.

The solution presented is an adaptation to smart cards and smart tokens. It enables the user to detect any malicious activity, whether software-based or firmware-based, so that only what the user wants to sign gets signed. Additionally, the same adaptation components realize secure biometric authentication.

Also, a method for entering secrets securely to the smart card or smart token is presented.