الخلاصة

عندما تريد المؤسسات توسيع مجال العملَ باستخدام الإنترنتِ، الشيء الأكثر أهمية الذي يجب أخذه بنظر الاعتبار كيفَ يجب أن تحمي أمنَ المعلومات مِنْ الهجوم أو الكشفِ مِن قِبل الشخص الغير مخوّل. والتحقُق مِنْ هويةِ المستعمل . كي نضمن أمن المعلومات والتحقق من الهوية، هناك أربعة متطلبات هي متطلبات الأمن وهي : السرية، سلامة المعلومات، التحقق وعدم الإنكار. عندما يصمم إي نظام اتصال هذه المتطلبات يجب أن تأخذ بنظر الاعتبار.

البنية التحتية للمفتاح المعلن (Public-Key Infrastructure) التقنية التي تحقق هذه المتطلبات.

نظام شهادةِ المفتاح المعلن يَعْملُ بامتلاك هيئة الشهادات (CA) لإصدار الشهادات الرقمية ذات المفتاح المعلن. كلا من (CA) و (PKI) تكون أجزاء مهمة في العديد من التطبيقات الشبكة الآمنة مثل التجارة ألالكترونية (E-commerce) و الحكومة ألالكترونية (E-government) والبريد الالكتروني الآمن (Secure Email) الخ.

إنّ هدفَ هذه الأطروحة هو تصميمُ نظام هيئة إصدار الشهادات الرقمية، هذا النظام يصدر شهادات المفتاح المعلن التي تُساعدُ في الاتصال الآمن والتحقُق الصحيح.هذه الأطروحة تستخدم طريقة جديدة تسهل عملية إلغاء الشهادة الرقمية . أيضا أعطاء هذه الشهادةِ بعض القوة وذلك باستعمال التشفير بطريقة المنحني الاهليلجي (ECC) بدلاً مِن طريقة RSA الذي هو مشاع الاستخدام حاليا . حيث أن الهدف الرئيسي من استخدام ECC هو لها قوة تشفير عالية نسبة إلى حجم المفتاح. هذه الشهادةِ تستخدم لحل مشكلة أمنَ المعلوماتِ والتحقُق مِنْ هويةِ المستعمل .

إنّ التصميمَ والتطبيقَ للنظامِ المُقتَرَح تم باستخدام لغات البرمجة مثل لغة PHP ولغة HTML بالإضافة إلى خادم قاعدةِ البيانات (MySQL Server) وخادم الويب (Apache Sever).

PDF created with pdfFactory trial version www.pdffactory.com

ABSTRACT

When the institutions want to extend the business scope by the Internet, the most important thing to consider how to protect the security of information from attack or disclosure by unauthorized person, and the authentication user identity. In order to make sure the security and the authentication, four main requirements are considered. These are Security Service: confidentiality, integrity, authentication and non-repudiation. When designing a communication system, the security services of this system must be defined. The Public-Key Infrastructures (PKI) is a technology that can meet these security services with its techniques and standards.

A public-key infrastructure system works by having a Certificate Authority (CA) for issuing public-key certificates. Both CA and PKI are crucial parts of many secure network applications such as E-commerce, E-government and Secure email.

The aim of this thesis is designing the Certificate Authority system, this system creates a public key certificate which helps in secure communication and proper authentication. This thesis uses a new approach that can contribute in facilitating the revocation of the certificates. Also gives these certificates some strength by using the Elliptic Curve Cryptography (ECC) instead of the (Rivest, Shamir and Adleman) RSA cryptography. Where the ECC has high cryptographic strength relative to key size.

This certificate tries to solve the security of information and authentication from user identity. The design and implementation of the proposed system are achieved using PHP and HTML programming languages besides MySQL database server and Apache web server.

PDF created with pdfFactory trial version www.pdffactory.com