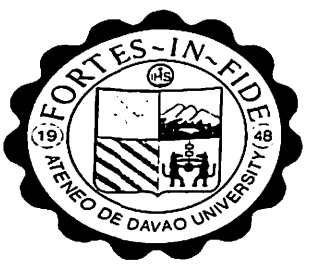
# DEVELOPING A WEB SERVICE BASED ARCHITECTURE FOR XML DOCUMENT AUTHENTICATION




BY

Lua, Jeffrey H.

Magbanua, Norma Niña Faye L.

Yap, Cherryln M.

SCHOOL OF ARTS AND SCIENCES
ATENEO DE DAVAO UNIVERSITY

MARCH 2006

# DEVELOPING A WEB SERVICE BASED ARCHITECTURE FOR XML DOCUMENT AUTHENTICATION

An Independent Research Presented to
The Faculty of the Computer Studies Division
Ateneo de Davao University

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Science in Computer Science

BY

Lua, Jeffrey H.

Magbanua, Norma Niña Faye L.

Yap, Cherryln M.

SCHOOL OF ARTS AND SCIENCES
ATENEO DE DAVAO UNIVERSITY

MARCH 2006

# TABLE OF CONTENTS

**Abstract**

The birth of the internet opened a lot of doors in how people communicate. It gave birth to e-commerce and online-transactions. With the advent of this new technology also come new threats that endanger the integrity of the information being passed around. One concern is determining whether a certain document has been tampered. To address this problem digital signatures, containing a hash value of the document and the time, are being embedded into digital documents. The hash value will be calculated using collision-free hash functions and one-way hash functions. This research will study the different document authentication techniques that are being used today and evaluate each of them. It will also look into some of the implementations of document authentication protocols that are now in use.

*Keywords:*
Document Authentication, Digital Signatures, Collision-Free Hash Function, One-Way Hash Functions, Cryptography

# CHAPTER 1

# INTRODUCTION

## 1.1 Background of the Study

The emergence of the internet paved the way for e-commerce. Nowadays small and medium size companies are looking at the possibility of moving their businesses to the internet. This made B2B *(business-to-business)* transactions and EDI *(Electronic Data Interchange)* possible. Doing business over the internet lowers cost and increases income for the company.

The eXtensible Markup Language *(XML)* is the universal format for structured documents and data on the Web. A lot of application, services and protocols uses XML because of the way it produces files that are easy to generate and read *(by a computer)*, that are unambiguous, and that avoid common pitfalls, such as lack of extensibility, lack of support for internationalization or localization, and platform-dependency.

Due to the rapid growth of companies using the internet for business transactions, new threats concerning security and authenticity of data and information arise. This is due to the simplistic nature of XML documents. These threats are now being addressed by different groups all over the world to make the internet a more secure avenue for transactions and e-commerce.

## 1.2 Statement of the Problem

Security has become a key requirement for the vast majority of current applications. As systems are being opened to the Internet, commercial traders,

financial institutions, service providers, and consumers are exposed to a variety of potential damages, which are often referred to as electronic risks. These may include direct financial loss resulting from fraud, theft of valuable confidential information, loss of business opportunity through disruption of service, unauthorized use of resources, loss of customer confidence or respect, and costs resulting from uncertainty.

The study seeks to address the general problem: How can the authenticity and integrity of an XML document be determined?

Specifically, it seeks to answer the following questions:

- What are the different methods being used in authenticating XML documents?
- How can the privacy of the document be maintained, even from the service provider?
- How can we guarantee long lived electronic documents over the years?
- How can we verify that a document is created in a certain point in time?

## 1.3 Objective of the Study

The general objective of this study is to develop a secure web service based architecture for authenticating XML documents.

The specific objectives are:

- To study the different techniques in authenticating XML documents.

- To develop a system that authenticates XML documents.
- To develop a system that is compliant to the W3C XML Digital Signature standard.

## 1.4 Scope and Limitation of the Study

The study will focus on developing a document authentication system. The study will focus on XML documents, even though these kinds of system can authenticate any digital document *(e.g. images, html)*.

The team will be using *Simple Hash Algorithm 1* (SHA 1) as the primary collision-free hash function because it has been thoroughly tested and remains to be the most secure hash function today. A successor to SHA1 is already available - SHA2, but it hasn't been thoroughly examined.

RSA will be used as the public-key encryption algorithm. RSA has been chosen because it is suitable for signing as well as encryption. RSA is still widely used in electronic commerce protocols. It is believed to be secure given the sufficiently long keys.

C# will be used in developing the application with Microsoft .net 2.0 and Microsoft SQL server for the database.

## 1.5 Significance of the Study

Software systems have functional requirements *(i.e., what services the system has to provide)*, and non functional requirements *(i.e., the quality the system must guarantee in the delivery of such services)*. Typical functional

requirements are business-specific services, and typical non functional requirements are security and performance.

Security is one of the major requirements for application that are open to the internet. In order to ease electronic risks and promulgate the deployment of information systems in open networked environments, applications must guarantee security features such as authentication, authorization, confidentiality, integrity, and non-repudiation. A particularly challenging issue is how to guarantee that long lived electronic documents can be verified over the years. To achieve this goal, it is crucial that a reliable document authentication system be made available.

During the last years the organizational and legal aspects of document authentication have become the subject of world-wide attention, both in academia and in the industry. Without document authentication the proponents neither can trust signed documents when the cryptographic primitives used for signing have become unreliable nor the proponents can solve the cases when the signer him/herself repudiates the signing, claiming that he/she has accidentally lost his/her signature key. Unfortunately, unlike physical objects, digital documents do not comprise the seal of time. Thus, the association of an electronic document uniquely with a certain moment of time is very complicated, if not impossible at all.

This study is significant to all business that are planning to explore the internet as a means of doing business and to those who are already engaged in e-commerce and online transactions