

# **Final Report**

## **Horse Racing System for 03-04 CSC 7251 Project I**

**Supervised by:** PROF. MICHAEL LYU

**Prepared by:** Wilson Ngan (02084880)

**Date:** 28-04-2003

## Table of Content

<b>1. INTRODUCTION .....</b>	<b>4</b>
<b>2. BACKGROUND.....</b>	<b>5</b>
2.1. WHAT IS COMPUTER SECURITY? .....	5
2.2. WHY IS TWO FACTORS AUTHENTICATION NEEDED?.....	5
2.3. ELECTRONIC TRANSACTIONS ORDINANCE (ETO) .....	6
2.4. WHAT IS A SMART HONG KONG IDENTITY CARD?.....	7
<b>3. PROJECT OBJECTIVES .....</b>	<b>9</b>
<b>4. OTHER ALTERNATIVES FOR ENHANCING SECURITY .....</b>	<b>10</b>
4.1. VIRTUAL PRIVATE NETWORKING (VPN) .....	10
4.2. RSA SECURE ID.....	10
4.3. BIOMETRIC AUTHENTICATION .....	10
<b>5. PROPOSED SYSTEM – HORSE RACING SYSTEM .....</b>	<b>12</b>
<b>6. CASE STUDY -- DAH SING BANK.....</b>	<b>13</b>
6.1. INTRODUCTION.....	13
6.2. E-CERT MEDIA TYPE .....	13
6.3. CLIENT INSTALLATION.....	14
6.4. LOGIN WITH E-CERT STORE AT FLOPPY BASE .....	15
6.5. LOGIN WITH E-CERT STORE AT SMART HKID .....	17
6.6. LOGIN WITH E-CERT STORE AT IKEY .....	18
6.7. DAH SING EBANKING VS HORSE RACING SYSTEM.....	20
<b>7. TECHNOLOGY AND SOFTWARE.....</b>	<b>21</b>
7.1. SOAP .....	21
7.2. WEB SERVICE.....	22
7.3. WEB SERVICES SERVER DEVELOPMENT TOOLKIT .....	22
7.4. CRYPTOGRAPHIC LIBRARY.....	24
7.5. FREE MARKER.....	26
7.6. ANT .....	27
<b>8. SYSTEM DESIGN OF HORSE RACING SYSTEM .....</b>	<b>28</b>
8.1. ARCHITECTURE OVERVIEW .....	28
8.2. WEB & APPLICATION SERVER DESIGN .....	29
8.3. WORKSTATIONS .....	34
8.4. TERMINALS .....	38
8.5. DATABASE SERVER .....	44
8.6. UDDI REGISTRY SERVER .....	46
8.7. FIREWALL .....	47
8.8. DATABASE SCHEME.....	48
8.9. UML DIAGRAM.....	50
8.10. WORKFLOW.....	52
<b>9. APPENDIX.....</b>	<b>54</b>
9.1. CODE TABLE OF RACESNUM.....	54
9.2. CODE TABLE OF HORSESNUM.....	54

9.3.	CODE TABLE OF POOL .....	54
9.4.	CODE TABLE OF FORMULA .....	54
9.5.	CODE TABLE OF BETUNIT.....	54
<b>10.</b>	<b>REFERENCE .....</b>	<b>54</b>

## **1. Introduction**

In today's environment, many applications need to ensure that only authorized individuals or customers gain access to critical devices or services offered. With the availability of password/PIN cracking tools and ready to use "sniffers", the basic authentication mechanism, using username/password or PIN combination, may no longer be adequate to withstand the test of secure authentication.

Other means of discovering password are aided by users' bad habits. Many users in general use easy-to-guess combinations such as birthday or phone number. Most of them never change password for a long period of time. Some of them even write their password or PIN down on label and stuck besides the computer. Some assign the same value to all their email accounts, online banking accounts and even to their ATM cards.

As the online transaction become more important, single factor authentication method may not be able to meet the security requirement. To solve the problem, two-factor authentication is proposed. Requiring two factors significantly enhances security because one factor authentication by itself may not be sufficient to perform authentication that can be relied on. Singapore has forced her financial institutions to applied two factors authentication on online banking system while Hong Kong Monetary Authorization also recommended two factors authentication for online banking system on March 2004.

## 2. Background

The wider adoption of e-commerce, corresponding sophistication of IT infrastructure and our present global economic downturn have raised and sharpened the customers' focus on e-commerce. Hong Kong has two critical success factors for developing e-commerce. They are mature legal system and IT infrastructure. Before discuss these two critical factors, we explore the necessary of computer security.

### 2.1. What is Computer Security?

Information is the most important asset any organization holds. It does not matter what form the information takes, either electronic, hardcopy or a person's knowledge. Whichever way the information is stored, the need for protection is of paramount importance, in order to provide business continuity, maximize business opportunities and mitigate potential risks to loss or damage. Information security has three important properties or requirements: integrity, confidentiality, and availability. Additional concepts that can be arguably kept separate are: Access Control, Non-repudiation, Availability, and Privacy.

Confidentiality	:Preventing unauthorized entities from accessing information or resources.
Integrity	:Ensure that data was changed by the authorized person, it is either not changed or any changes are detectable.
Authentication	:Making sure that entities are who/what they claim to be.
Access Control	:Ensure that entities can only access services, resources, or information that they are authorized for.
Non-repudiation	:One may not deny his/her actions.
Availability	:Ensure resource can be accessed by authorized users only. While this goes beyond security, security is expected to address denial of service attacks.

### 2.2. Why is Two Factors Authentication needed?

**Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.**

*Ronald L. Krutz, The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*

Single-factor authentication usually consists of "something you know". However, generally, these could be susceptible to attacks that could compromise the security of the application. Some of the more common attacks can occur at little or no cost to the perpetrator and without detection.

One example of single factor authentication is amply demonstrated by fake website for banking system. On 27 Dec 2003, DBS Group Holdings, Singapore's largest bank, has notified police and banking regulators of a fake website that has sprung up under the DBS name, purporting to serve customers of its Hong Kong

operations. It is the fourth financial institution in Hong Kong to report a phony website, after Bank of China, HSBC Holdings and Schroders all reported similar fakes last year.

Choosing the appropriate identification and authentication tools depends on the channels through which an organization wishes to provide its services, the flexibility that it wishes to provide its users and customers alike, and the perceived risks.

Y	<b>Subject must prove something he knows (e.g. password)</b>
Y	<b>Subject must prove something he has (e.g. smart card)</b>
Y	<b>Subject must prove something he are (e.g. fingerprint)</b>

*Shon Harris, Mike Meyers' CISSP(R) Certification Passport.*

Specifically, there are three user authentication methods:

- Something you have - this can include a key to a door or a token card;
- Something you know - passwords or PINs may be classed in this category;
- Something you are - this area includes biometric authentication such as fingerprints, voice recognition, retina or iris scans.

Two-factor authentication is based on “something you know”, and “something you have” or “something you have” — providing a much more reliable level of user authentication than reusable password. In addition to reducing the risk of unauthorized access, two-factor authentication also provides institutions with a foundation to enforce electronic transactions and agreements (Non-repudiation). First, effective authentication provides the basis for validation of parties to the transaction and their agreement to its terms. Second, it is a necessary element to establish authenticity of the records evidencing the electronic transaction should there ever be a dispute. Third, it is a necessary element to establish the integrity of the records evidencing the electronic transaction. All of these elements promote the enforceability of electronic agreements.

An effective authentication method should have customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with existing systems and strategic plans of the organization.

No matter what type of two-factor authentication model is used, the organization should be sensitive to the fact that proper implementation is key to the reliability and security of the system. For example, a poorly implemented two-factor system may be less secure than a properly implemented single-factor system because of weak organizational policy, procedures or standards. This is so, because the human element is the weakest link in any security application or system.

### **2.3. Electronic Transactions Ordinance (ETO)**

To promote the development of electronic commerce, the Hong Kong Government launched an Electronic Service Delivery (ESD) scheme. The first phase

of ESD will be implemented in the latter half of 2000, public services will be available on-line, 24 hours a day, seven days a week.

In parallel, the Government introduced the Electronic Transaction Bill on July 14, 1999 to address public concerns about the security and certainty of electronic transactions, e.g., the legal status of electronic records and digital signatures, authentication of the parties to electronic transactions, the confidentiality and integrity of electronic messages transmitted over open communications networks and non-repudiation of electronic transactions. To provide a secure and trusted environment for the conduct of electronic transactions, Government has established a public key infrastructure (PKI) in Hong Kong through the Hongkong Post, which started to provide public certification services on a non-exclusive basis by the end of 1999. With the issue of digital certificates by certification authorities (CAs) and through the use of digital signatures and public/private key encryption, individuals and businesses will be able to establish the identity of the opposite party in electronic transactions, authenticate electronic messages received, ensure that the confidentiality and integrity of electronic messages have not been breached and safeguard against the repudiation of electronic transactions.

#### 2.4. What is a Smart Hong Kong Identity card?



Figure 1. The front and back of a smart ID card

With effect from 23 June 2003, the Government of the HKSAR starts to issue a new generation of identity cards (Shown in Figure ) in the form of smart cards. The new smart identity card bears the following characteristics:

1. The new identity card takes the form of a smart card with the size of a standard credit card;
2. The card is produced by polycarbonate, a durable and secure base material with strong resistance to environmental influences as well as mechanical, chemical and thermal stress;
3. The card is embedded with an integrated circuit, or a "chip" which has the capacity of storing and processing data.
4. The card is embedded with card applications: Immigration Applications, e-Cert Application, Library Card Application and Driving Licence-related Functions

Under the current policy, only the Hongkong Post e-Cert can be loaded on the card and accessed by using e-Cert Application.

### **What is e-Cert?**

Hongkong Post e-Cert can be regarded as a user's "online identity card" for authentication purposes. It ensures integrity, confidentiality and non-repudiation of the data transmitted in an electronic transaction. The issue of e-Cert involves a trusted organisation (the Hongkong Post Certification Authority) to verify an e-Cert applicant's identity. With an e-Cert, cardholders are able to prove their identity as well as digital signatures and can send encrypted messages. The recipient could check with the certification authority to determine if the e-Cert and digital signature attached to it are valid and genuine. The validity period of the e-Cert on smart ID card is three years. With this smart ID card introduction offer, residents can enjoy free use of e-Cert for the first year. After this initial trial period, residents can continue using the e-Cert by paying an annual subscription fee. For details of the annual subscription fee, please [click here](#).

### **Usage of e-Cert**

The key to enjoying the full "anytime, anywhere" benefits of e-commerce is to ensure that the online trading environment is secure and reliable. Hongkong Post e-Cert may be used for public and commercial purposes such as secure email communication; e-government services; online entertainment, stock trading and payment; as well as e-banking services.



### 3. Project Objectives

**Europe has been at the forefront of smart card technology, with the number of cards in circulation estimated at around 50 million, accounting at present for more than 95 percent of the global total.**

*From Banking and Finance on the Internet; Mary J. Cronin ; John Wiley & Sons, Inc., 1997*

**A smart card, about the size of a credit card, can contain an electronic purse that the user fills with e-cash and then uses for making purchases**

*Cybercorp; James Martin ; Amacom, 1996*

Mary J. Cronin and James Martin pointed out that smart card are useful for electronic transaction. Providing e-banking services through different channels using a flexible, portable two-factor authentication model, one of the most cost-effective solutions available is smart cards solution.

The objective of Horse Racing system is to demonstrate how to enhance the security of e-Commerce by applying several well-proven technologies and the e-Cert embedded in Smart HKID card. These well-proven technologies include Web Services, PKI and Smart Card.

## 4. Other Alternatives for Enhancing Security

### 4.1. Virtual Private Networking (VPN)

VPN's allow you to use the public Internet to securely connect remote offices and remote employees at a fraction of the cost of dedicated, private telephone lines, such as frame relay. There are two major uses for VPNs. The first is to connect two or more geographically separated networks, such as those at a main office and a remote branch office. The second is to allow employees or authorized users to access a network from a remote PC, such as a traveling laptop or home computer. Both of these uses involve providing authorized users with access to protected network resources. The following are some of the basic VPN concepts:

### 4.2. RSA Secure ID

The RSA SecurID system is a well-recognized two-factor user authentication solution. Thousands of organizations deployed this system and protect valuable network resources. An RSA SecurID authenticator (Shown in Figure 2) functions like an ATM card for your network, requiring users to present identify themselves with two unique factors — something they know and something they have — before they are granted access. Each end user is assigned an RSA SecurID authenticator which generates a new, unpredictable code every 60 seconds. The user combines this number with a secret PIN to log into protected resources.

This is a highly secure solution but too expensive for corporation with large customer base such as banks. Thus, an economic two-factor user authentication solution over Internet is necessary for future.



Figure 2. Different RSA SecurID authenticator

### 4.3. Biometric authentication

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and

transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

## 5. Proposed System – Horse Racing System

**The question is not so much how to make profits today but how to spot future profitability.**

*Net Profit; Peter S. Cohan ; Jossey-Bass, 1999 y*

Without improving the functionality of system, changing from web-base system to a web service system seems make no profits. But Peter S. Cohan points out our focus should be shift to future profitability. Imagine that when every web-base system with a web service interface, a new business model will be evolved.

Horse Racing System is a kind of web service system. It allows any application interact with web service server over protocol SOAP. The client application may be a Windows application, Java application or even server application. With the Smart HKID card supports, computer security CIA – Confidentiality Integrity, Authentication can be applied with Non-repudiation.

The detail design of Horse Racing System can refer to Section 8 System Design of Horse Racing Sytem.

## **6. Case Study -- Dah Sing Bank**

### **6.1. Introduction**

Dah Sing e-banking is the first Bank that supports Smart ID card as their authentication process over Internet. It is an example two-factor user authentication approach. It brings extra security and protects customers from unauthorized access to their accounts.

In physical world, when customers make transactions with their accounts, they have to present a passbook together with their authorized signature. Using a digital certificate is similar to presenting a passbook together with your HKID at the bank counter. Besides, you are still required to submit your Personal Identification Number (PIN) for verification.

### **6.2. e-Cert Media Type**

The e-Cert (and associated key pair) on Smart HKID card cannot be copied to other storage media. Hongkong Post offers an optional service to backup your smart ID card e-Cert on a floppy disk at the time you submit your e-Cert application. Each floppy disk costs HK\$10. With the back-up copy, you can then import your e-Cert into the browser of your personal computer and access the e-Cert directly (if the smart card reader has not been installed yet). The backup e-Cert floppy disk will be delivered to your address by Recorded Delivery service.

Other than Smart HKID card and floppy, user can carry that confidence with you and safeguard all of critical information by using iKey, a new storage media, offered by Hongkong Post CA. The iKey is an USB-based secure token designed for cost-effective and easy-to-use control and protection for your private/public key-pairs and digital certificates. And Dah Sing e-banking supports e-Cert stored on three different types of media. (Show in Figure 3)



Figure 3 Select media type that contain e-Cert

### 6.3. Client Installation

To access the e-Cert application on Smart HKID card, software must be installed. The distribution of client software is through browser. Within the HTML page, an embedded object is declared. Browser will download the software client from server and verify it. The Dah Sing eBanking's client software located at their web server <https://dahsing.com/eBank/js/P11Applet.cab> (Show in Figure 4)

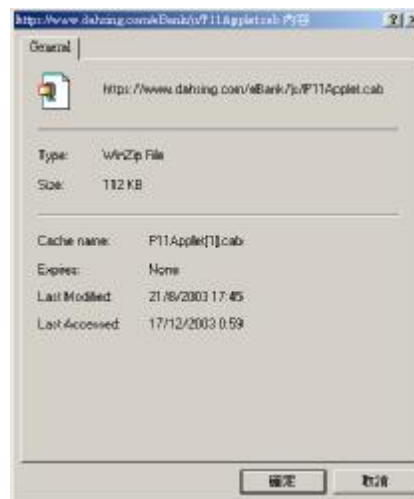


Figure 4 CAB file(Client Software)

During the installation and verification process by browser, a popup window (Show in Figure 5) will ask for authorization of installation. We find that this CAB is signed by SecureNet Asia Limited. To complete the installation process, press Y to

install. Without the proper software installation, user cannot access the e-Cert on any media.



Figure 5 Authorization Request from SecureNet Asia Limited

#### 6.4. Login with e-Cert store at Floppy Base

To login system by floppy base e-Cert, user have to enter password for digital certificate, PIN for e-banking account and the file path of certification by clicking the button “請選擇檔案” (Shown in Figure6). And then click button “登入”.



Figure 6 Login with e-Cert store at Floppy Base

Client software will use the password to open the digital certificate in PKCS12 format. As the PKCS12 format support storing more than one pair of certificate and

user may acquire another digital certificate from other CA , TrustNet Applet (Show in Figure 7) may ask for selecting the digital identity for login.



Figure 7 Selecting the digital identity

After successfully open and select the digital identity, client software will sign the challenge embedded in HTML page (Shown in Figure 6). The signed content of HTML page (Shown in Figure 8) is a challenge. This challenge is a numeric value made up of 22 characters that may be the result of a hashing function using the date, time and value of the transaction itself. It is store in field named "text" and the signature on this challenge will be store at field named "sign". Although the signature algorithm does not stated in HTML page, the signature algorithm most likely is SHA1-RSA.

```
<tr>
  <td height="35" width="22%">
    <div align="right"><font face="Arial, Helvetica, sans-serif" size="2"><B>數碼證書密碼
  </B></font></div>
  </td>
  <td height="35" width="2%">&nbsp;</td>
  <td height="35" width="30%">
    <input type=password name=eCertPassword size="20">
    <input type=hidden name=cert size="1000">
    <input type=hidden name=epin size="50">
    <input type=hidden name=key>
    <input type=hidden name=lang value="CHI">
    <input type=hidden name=ipaddress>
    <input type=hidden name=IKSStatus size="3">
    <input type=hidden name=text value="1071591611520620538783">
    <input type=hidden name=sign value="">
  </td>
  <td height="35" width="2%">&nbsp;</td>
  <td height="35" width="44%"></td>
</tr>
<tr>
  <td height="35" width="22%">
    <div align="right"><font face="Arial, Helvetica, sans-serif" size="2"><B>請選擇數碼證書
  </B></font></div>
  </td>
  <td height="35" width="2%">&nbsp;</td>
  <td height="35" width="30%">
    <input type=text name=txtFile>
  </td>
  <td height="35" width="2%">&nbsp;</td>
```



```

<td height="35" width="44%"><input name=btnFile onClick="javascript:applet_show_dialog(); "
type=button value="請選擇檔案"></td>
</tr>
<tr>
<td height="35" width="25%">
<div align="right"><font face="Arial, Helvetica, sans-serif" size="2"><b>網上理財密碼</b>
</font></div>
</td>
<td height="35" width="1%">&nbsp;</td>
<td height="35" width="30%">
<input type=PASSWORD name="pin" size="20" MAXLENGTH="6">
</td>
<td height="35" width="1%">&nbsp;</td>
<td height="35" width="43%"><a href="javascript:validateAndSubmit()"></a></td>
</tr>

```

Figure 8. HTML of Login Page (Using e-Cert store at Floppy Base)

As server generates the challenge for this HTTP session, server can verified the signature against their challenge record in database. After successfully verification, the authentication is complete.

## 6.5. Login with e-Cert store at Smart HKID

To login system by using e-Cert embedded in Smart ID card. Users simply insert their Smart HKID card into smart card reader. Enter password for e-Cert and PIN for e-banking account into login page (Shown in Figure 9)



Figure 9 Login with e-Cert store at Smart HKID

Client software use the password to access e-Cert application and create a digital signature on this challenge. Similar to floppy base HTML page, this HTML page (Show in Figure 10) has field named “text” contains the challenge which is a numeric value made up of 22 characters. The field named “sign” will store the signature value and post to server.

```

<tr>
  <td height="35" width="22%">
    <div align="right"><font face="Arial, Helvetica, sans-serif" size="2">
      <b>智能身份證密碼</b></font></div>
    </td>
    <td height="35" width="2%">&nbsp;</td>
    <td height="35" width="30%">
      <input type=password name=spin size="20">
      <input type=hidden name=cert size="1000" >
      <input type=hidden name=text value="1071593261920437400658">
      <input type=hidden name=sign value="">
      <input type=hidden name=epin size=50>
      <input type=hidden name=key>
      <input type=hidden name=lang value="CHI">
      <input type=hidden name=ipaddress>
      <input type=hidden name=smidlogin value="Y">
    </td>
    <td height="35" width="2%">&nbsp;</td>
    <td height="35" width="44%">&nbsp;</td>
</tr>
<tr>
  <td height="35" width="25%">
    <div align="right"><font face="Arial, Helvetica, sans-serif" size="2"><b>網上理財密碼</b>
    </font></div>
  </td>
  <td height="35" width="1%">&nbsp;</td>
  <td height="35" width="30%">
    <input type=PASSWORD name="pin" size="20" MAXLENGTH="6">
  </td>
  <td height="35" width="1%">&nbsp;</td>
  <td height="35" width="43%"><a href="javascript: validateAndSubmit()"></a></td>
</tr>

```

Page 10. HTML of Login Page (Using e-Cert store at Smart HKID)

## 6.6. Login with e-Cert store at iKey

The last option is to use the e-Cert stored on iKey (Shown in Figure 11). iKey is a two factor authentication device produced by Rainbow Technologies for use with a wide range of products and solutions. It can plug into a standard USB port, and is small and robust enough to carry on a key-ring iKey can also be used to encrypt files and to digitally sign emails or documents.



Specification:-

1. Support Hongkong Post e-Cert, storage of X.509 certificate, private/public keys;
2. 32K secured storage; USB 1.1 / 2.0 compliant;
3. On-board 1024-bit RSA algorithm, key signing and key pair generation;
4. PKCS#11 and Microsoft CAPI middleware
5. Supports MS IE, Outlook and Outlook Express.

Figure 11 Specification of iKey by Rainbow

To login system by using e-Cert embedded in iKey. Users simply insert their iKey into USB slot. Enter password for e-Cert and PIN for e-banking account into login page (Shown in Figure 12)

Similar to previous authentication mechanism, client software uses the password to access iKey and create a digital signature on this challenge. The signature will be store at field named “sign” and then post to server. After success verification, user is authentication.



Page 12. HTML of Login Page (Using e-Cert store at iKey)

### 6.7. Dah Sing ebanking vs Horse Racing System

	Dah Sing eBanking	Horse Racing System
Client Application	Internet Explorer	Windows Application
Client Authentication	Challenge-response mechanism	Challenge-response mechanism
Server Authentication	HTTPS	Challenge-response mechanism
Data Exchange	Runtime session key	Runtime session key
Mechanism	Two-factor	Two-factor
Integration Difficulty	Difficult	Easy
Development Language	Server Side: Java Client Side: Applet + DLL	Server Side: Java Client Side: VB + VC + DLL

*Table 1 Feature comparison between Dah Sing eBanking and Horse Racing System*

In summary, Horse Racing System can provide the same security level as Dah Sing ebanking system. The more important is that the authentication mechanism implemented by Horse Race System has more flexibility on migration and system integration.

## 7. Technology and Software

Many technologies and software have been used in Horse Racing System. Before we further discuss the system design of Horse Racing System, we discuss those technologies and software one by one.

### 7.1. SOAP

The Simple Object Access Protocol (SOAP) is designed to invoke remote applications independent of platform and programming language. It is important for application development to allow applications to communicate over the Internet, irrespective of the platform on which the application is running. Today's applications communicate using Remote Procedure Call (RPC) mechanisms between objects using protocols like DCOM and CORBA. However, HTTP was not really designed to accommodate the sophisticated interactions needed when using these RPCs. Because an RPC carries a request to do something rather important, RPC represents a compatibility and security vulnerability that firewalls and proxy servers will normally block. The challenge then is to allow this kind of complex application interaction using an RPC without compromising security and without sacrificing platform-agnostic advantages. SOAP is the protocol for packaging these requests when sending method calls over HTTP. SOAP makes it possible to communicate between applications running on different operating systems, with different technologies and programming languages all in play. In this chapter covers the nuts and bolts of SOAP.

## **7.2. Web Service**

### **7.2.1. What is Web Service?**

A Web service is a component-based, self-describing application based on an architecture of emerging standards. Other technologies like CORBA, DCOM, and Java RMI have all targeted the same objective: deliver application functionality as a service-oriented component in a distributed and heterogeneous environment. This chapter introduces readers to the concepts of Web services and how they relate to application development, whether the applications leverage XML or not. The chapter starts with the basic concepts of Web Services Architectures, SOAP, WSDL, and UDDI.

### **7.2.2. What is WSDL?**

WSDL is the other moving part of a Web Services Architecture, which defines what SOAP calls and responses should look like, and helps Web service calling agents define what an interface should be to a specific Web service.

### **7.2.3. What is UDDI?**

Universal Description, Discovery and Integration (UDDI) is an industry specification for publishing and locating information about Web services. It defines an information framework that enables you to describe and classify your organization, its services, and the technical details about the interfaces of the Web services you expose. The framework also enables you to consistently discover services, or interfaces of a particular type, classification, or function. UDDI also defines a set of Application Programming Interfaces (APIs) that can be used by applications and services to interact with UDDI data directly

## **7.3. Web Services Server Development Toolkit**

### **7.3.1. Java Web Services Developer Pack (Java WSDP)**

The Java Web Services Developer Pack (Java WSDP) is a free integrated toolkit developed by Sun Microsystems that allows Java developers to build and test XML applications, Web services, and Web applications with the latest Web service technologies and standards implementations. Technologies in Java WSDP include the Java APIs for XML, Java Architecture for XML Binding (JAXB), JavaServer Faces, Web Services Interoperability Sample Application, XML Security, JavaServer Pages Standard Tag Library (JSTL), Java WSDP Registry Server, Ant Build Tool, and Apache Tomcat container.

### 7.3.2. Apache Axis

Axis is a generalized SOAP message handling system that is focused on providing developers with a rich set of tools and infrastructure for developing and consuming Web Services. This open-source tool contains all the basic elements a developer would need to rapidly consume, build, deploy, and host a Web Service. Axis strikes a nice balance between power and complexity, allowing developers to quickly build Web Services with a relatively short learning curve while still allowing more advanced customization of message processing, type mapping, and so on. In this chapter, the fundamentals of the Axis architecture are covered, taking an in-depth look at how the Axis engine processes requests and responses. The chapter will also examine some of the goals of the architecture and how these goals influenced the solution that was ultimately implemented. It will also discuss each of the deployment models that are supported by Axis. Specifically, the chapter will look into how developers can customize their Web Service configuration via deployment descriptors

### 7.3.3. Web Services Toolkit (WSTK)

Other Java WSDP, Web Services Toolkit (WSTK) developed by IBM is another choice. WSTK has evolved into the Emerging Technologies Toolkit (ETTK). ETTK is a software development kit for designing, developing, and executing emerging autonomic and Web service technologies. The ETTK provides an environment in which to run emerging technology examples that showcase recently announced specifications and prototypes from IBM's emerging technology development and research teams. In addition, it provides introductory material to help developers easily get started with development of autonomic technologies and Web services.

### 7.3.4. Microsoft's .NET Framework

The .NET Framework comes with all of the building blocks for Web services built right in. Essentially, any server with the .NET Framework and IIS installed is ready to provide Web services. Furthermore, .NET carefully balances the need for making Web services easier to create, deploy, and maintain with the requirement that developers still be able to go under the hood and do more advanced techniques

### 7.3.5. Summary of Development Toolkit

Package Name	Vendor	Server
Java Web Services Developer Pack (Java WSDP)	Sun	Tomcat
Emerging Technologies Toolkit (ETTK)	IBM	Websphere
Apache eXtensible Interaction System (AXIS)	Apache	Apache
Microsoft's .NET Framework	Microsoft	IIS

Table 2 Summary of Web Service Development Toolkit

In Horse Racing System, we select the Java WSDP as the Web Service Development Toolkit. It is because it is FREE and provides complete document. Moreover, the web application can be easily integrate with servlet and JSP.

## **7.4. Cryptographic Library**

To perform cryptographic operation, cryptographic library is required. The following list of cryptographic libraries are famous over the world and widely used. To support Horse Racing System, more than one cryptographic library may be used.

### **7.4.1. Openssl**

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric A. Young and Tim J. Hudson. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

Other than cryptographic Library, OpenSSL is a robust and has rich refined set of command line tools. Therefore, we will use it in application server.

### **7.4.2. Java Cryptography Extension (JCE)**

The Java Cryptography Extension (JCE) provides APIs for performing cryptographic operations in Java code. Essentially, the JCE lets us scramble and unscramble data, annotate code and data with information that lets others verify it came from us, verify the integrity of data sent from others, and perform administrative operations associated with cryptographic primitives like ciphers, secret keys, etc. We'll discuss these in more detail later, but first we need to introduce some basic terminology used when doing cryptography, understand how the JCE relates to other Java security APIs, and get an overview of the JCE's architecture.

### **7.4.3. Bouncy Castle Crypto Package**

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. The package is organized so that it contains a light-weight API suitable for use in any environment (including the newly released J2ME) with the additional infrastructure to conform the algorithms to the JCE framework. Bouncy Castle Crypto package has a light-weight cryptography API, a clean room implementation of the Sun Java Cryptography Extension (JCE) and a cryptographic provider for the JCE and the JCA.



#### 7.4.4. Microsoft CryptoAPI

The Cryptography API is implemented as an application-level system that Win32 applications may call for cryptographic services. The applications are thereby insulated from the business of providing their own algorithms for such things as encryption and hashing. Against that, the applications are limited to whatever cryptographic services happen to be available in the current configuration of the CryptoAPI system.

The CryptoAPI system is built in parts. An interface layer is exposed to the client applications. Underneath are drivers that do the actual work of providing the cryptographic services. Each such driver is called a Cryptographic Service Provider (CSP). Microsoft itself supplies some CSPs with the CryptoAPI system. As it is built in parts of Windows System, we will use it in our workstation.

#### 7.4.5. Summary of Cryptographic Library

	Command Line	Platform	Language	CA support
OpenSSL	Yes	Windows, Unix, Linux, MasOS, VMS, OS2	C	Yes
JCE	No	Follow Java	Java	No
Bouncy Castle	No	Follow Java	Java	Yes
Crypto API	No	Windows	VC	Yes

Table 3 Summary of Cryptographic Library

## 7.5. Free Marker

The J2EE relies heavily on JavaServer Pages (JSP) to bridge the gap between EJB and HTML code, placing JSPs at the key boundary between data and presentation. However, JSP falls short of its intended purpose. For one thing, advocates of the model-view-controller design pattern still find fault in JSP's architecture. FreeMarker, an alternative to JSP. FreeMarker is a "template engine"; a generic tool to generate text output (anything from HTML or RTF to auto generated source code) based on templates. It is 100% written in Java.

FreeMarker is designed to be practical for the generation of HTML Web pages, particularly by servlet-based applications following the MVC (Model View Controller) pattern. The idea behind using the MVC pattern for dynamic Web pages is that you separate the designers (HTML authors) from the programmers. Everybody works on what they are good at. Designers can change the appearance of a page without programmers having to change or recompile code, because the application logic (Java programs) and page design (FreeMarker templates) are separated. Templates do not become polluted with complex program fragments.

Although FreeMarker has some programming capabilities, it is not a full-blown programming language like PHP. Instead, Java programs prepare the data to be displayed, and FreeMarker just generates textual pages that display the prepared data using templates.



Figure 12 Overview of FreeMarker Flow

FreeMarker is not a Web application framework. It is suitable for a component in a Web application framework, but the FreeMarker engine itself knows nothing about HTTP or servlets. It simply generates text. As such, it is perfectly usable in non-web application environments as well. Note, however, that we provide out-of-the-box solutions for using FreeMarker as the view component of Model 2 frameworks (e.g. Struts), which also let you use JSP taglibs in the templates.

## 7.6. *Ant*

Apache Ant is a Java-based build tool. In theory, it is kind of like Make, but without Make's wrinkles.

Makefiles are inherently evil as well. Anybody who has worked on them for any time has run into the dreaded tab problem. "Is my command not executing because I have a space in front of my tab!!!" said the original author of Ant way too many times. Tools like Jam took care of this to a great degree, but still have yet another format to use and remember.

Ant is different. Instead of a model where it is extended with shell-based commands, Ant is extended using Java classes. Instead of writing shell commands, the configuration files are XML-based, calling out a target tree where various tasks get executed. Each task is run by an object that implements a particular Task interface.

Granted, this removes some of the expressive power that is inherent by being able to construct a shell command such as ``find . -name foo -exec rm {}``, but it gives you the ability to be cross platform -- to work anywhere and everywhere. And hey, if you really need to execute a shell command, Ant has an `<exec>` task that allows different commands to be executed based on the OS that it is executing on.

## 8. System Design Of Horse Racing System

### 8.1. Architecture Overview

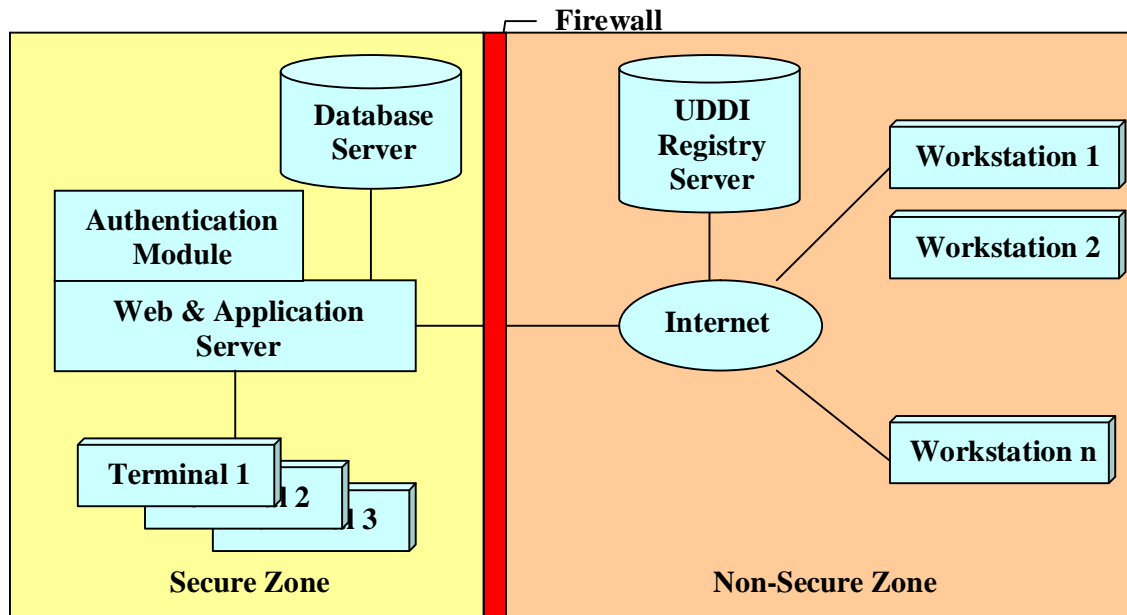


Figure 13 Architecture Overview

Horse Racing System is a 3-tier system and can be divided into two zones. They are Secure Zone and Non-Secure Zone. These two zones are separated by using software Firewall.

In Secure Zone, the security requirement will be less restricted. It is because environment within Secure Zone is under control. Hardening, policy and other physical security can be considering as feasible solution to enhance security level. Within the secure zone, web & application server, database server and terminals are setup. The Web & Application server will be the single point of contact with Internet. Database server and terminals are unreachable from outside.

In Non-Secure Zone, the security requirement will be highly important. Privacy, data integrity, authentication and non-repudiation are four basic requirements. Within non-secure zone, UDDI registry server and workstation are setup.

## 8.2. Web & Application Server Design

### 8.2.1. System Overview

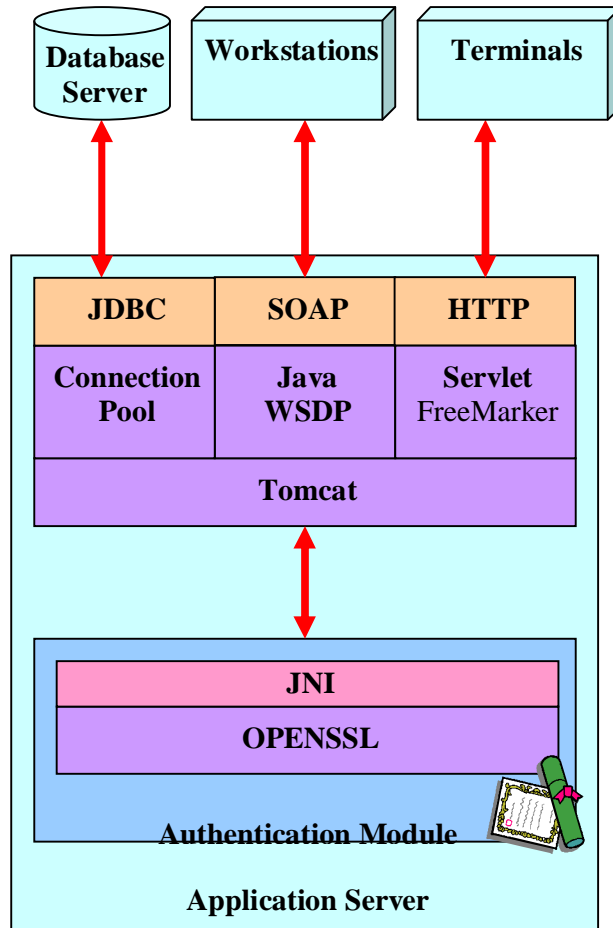


Figure 14 Application Server Overview

Application Server is the most complicated component within Horsing Racing System. It interacts with Database Server, Workstations and Terminals using JDBC, SOAP, and HTTP corresponding. Other than distributed component, an Authentication Module for e-Cert is embedded in Application Server and communicates with Application Server through JNI.

Application Server contains the logic and workflow of Horsing Racing System. It acts as the middle tire among 3 tires.

## 8.2.2. System Requirement

Application is design to run on Windows system. It is recommended to run on Windows 2000 Professional SP4. Several software are required for application server. They are as following:

1. Java™ 2 SDK, Standard Edition (jdk1.4.2\_03)
2. Java Web Services Developer Pack (Java WSDP)
3. Apache Commons Logging module 1.0.3 or above
4. Apache Commons DBCP 1.1 or above
5. Apache Commons Pool 1.1 or above
6. Jakarta log4j 1.2.8 or above
7. Openssl 0.9.7 or above
8. Oracle JDBC Driver

## 8.2.3. Web Service Server

Web Service Server provides two services over SOAP. They are viewing balance and bet. To obtain these services, customers have to complete mutual authentication and get a session key before proceed. (Detail please refers to Section 10.8.1 Mutual Authentication). After exchange session key, data are available exchange under a secure channel (Detail please refers to Section 10.8.2 Secure Data Exchange). Each session will be cleaned up after disconnect (Detail please refers to Section 10.8.3 Session Clean Up). In order to fulfill the above requirement, five web service interfaces are necessary in Horse Racing System. They are as following:

- 1.) GetChallenge – This API will trigger server to generate a challenge for login purpose and save into database along with session id. A base 64 encoded server challenge and session id will be return.
  - [in] void
  - [out] String sessionID – Session ID for each connection
  - [out] String b64ServerChallenge – Server challenge for authenticating client
- 2.) Login – This API will submit the login request to server. If server authenticate client successfully, session key encrypted by server public key and digital signature for client challenge will be returned. If authentication failure, empty string will be return.
  - [in] String sessionID – Session ID for each connection
  - [in] String b64Signature – Digital signature for server challenge
  - [in] String b64ClientChallenge – Client challenge for authenticating server
  - [out] String b64RSAEncryptSessionKey – Encrypted Session Key for data exchange
  - [out] String b64Signature – Digital signature for client challenge
- 3.) ViewBalance – This API trigger server to query the balance and return to balance to workstation.

- [in] String sessionID – Session ID for each connection
- [in] String b64TriDesEncryptInstruction – Session key encrypted instruction
- [out] String b64TriDesEncryptBalance – Session key encrypted balance

4.) Bet – This API submits the bet request to server and create an transaction record at database.

- [in] String sessionID – Session ID for each connection
- [in] String b64TriDesEncryptInstruction – Session key encrypted instruction
- [out] String b64TriDesEncryptResult – Session key encrypted transaction ID

5.) Logout – This API end the connection and clear the session information for database.

- [in] String sessionID – Session ID for each connection
- [in] String b64TriDesEncryptInstruction – Session key encrypted result

#### 8.2.4. Web & Application Server

HTTP Server provides management function for administrators. In Horse Racing System, there are 7 types of administrators. Each type of administrator is allowed to manage its scope only.

Administrator Type	Scope	Value
Stable Administrator	Stable	0x01
Stable Owner Administrator	Stable Owner	0x02
Race Administrator	Race	0x04
Jockey Administrator	Jockey	0x08
Horse Administrator	Horse	0x10
Trainer Administrator	Trainer	0x20

Table 4. Scope and value for different administrator type

For the detail of each Scope, please refer to Section 8.4 Terminals.

#### 8.2.5. Connection Pool

Applications that make use of databases often need to frequently obtain connections to the database. For example, a popular website that is serving out information from a back-end database may need to obtain a database connection for each client who is requesting a page with their browser. To ensure the application is capable of responding to each client fast enough we need to profile the time spent performing each of it's tasks. One of the most expensive tasks involving accessing databases is the initial creation of the connection. Once the connection has been made the transaction often takes place very quickly. This is where the connection pool comes in, by retaining a pool of already-opened connections so the application can

simply grab one when it needs to, use it, and then hand it back, without the long wait for the initial creation of the connection.

Parameter	Description
defaultAutoCommit	The default auto-commit state of connections created by this pool.
maxActive	The maximum number of active connections that can be allocated from this pool at the same time, or zero for no limit.
maxIdle	The maximum number of active connections that can remain idle in the pool, without extra ones being released, or zero for no limit.
minIdle	The minimum number of active connections that can remain idle in the pool, without extra ones being created, or zero to create none.
maxWait	The maximum number of milliseconds that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely.

Table 5. Configuration Parameter of Connection Pool

### 8.2.6. e-Cert Authentication Module

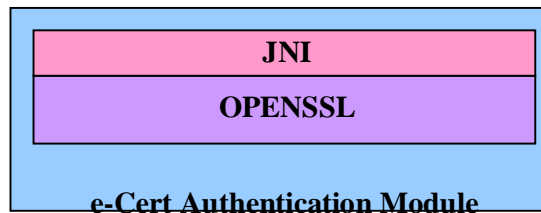


Figure 15 Authentication Module Overview

e-Cert Authentication Module is divided into two components. They are OpensslWrapperCOM and CryptoWrapperJNI. Web Service Server can perform cryptographic operation directly through the interface provided by JNI.

#### **OpensslWrapperCOM**

Openssl wrapper COM library provides a COM API for Openssl Library. Windows application developed by Visual Basic or Visual C++ or VBA can call it and perform cryptographic operation easily.

#### **CryptoWrapperJNI**

Crypto wrapper provides a Java API for OpenWrapperCOM library. Java application can call it and perform cryptographic operation easily.

This major advantage of divide e-Cert Authentication Module into two components is the OpensslWrapperCOM library can be reused in the future and easy



---

for testing. The problem such as memory leakage or Java VM core dump caused by JNI can be isolated to diagnose.

### 8.2.7. CRL Verification for Hongkong Post e-Cert

Hongkong Post updates and publishes the following Certificate Revocation Lists (CRLs) containing information of suspended or revoked e-Certs and Bank-Certs 3 times daily at 09:15, 14:15 and 19:00 Hong Kong Time (i.e. 01:15, 06:15 and 11:00 Greenwich Mean Time (GMT or UTC)):-

- Y Partitioned CRLs that contain Information of suspended or revoked certificates in groups. Each of the partitioned CRLs is available for public access at a location (URL) specified in the "CRL Distribution Points" field of each certificate issued. For e-Cert (Personal), the URL is in the form of [http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1\\_<xxxxx>.crl](http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1_<xxxxx>.crl), where <xxxxx> is a string of five alphanumeric characters. For other types of e-Cert and Bank-Cert, the URL is <http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL2.crl>
- Y Full CRL that contains Information of all suspended or revoked certificates. The Full CRL is available at :  
<http://crl1.hongkongpost.gov.hk/crl/eCertCA1CRL1.crl>; or  
<ldap://ldap1.hongkongpost.gov.hk> (port 389, cn=Hongkong Post e-Cert CA 1 CRL1, o=Hongkong Post, c=HK);

Under normal circumstances, Hongkong Post will publish the latest CRL as soon as possible after the update time. Hongkong Post may need to change the above updating and publishing schedule of the e-Cert CRL without prior notice if such changes are considered to be necessary under unforeseeable circumstances.

## 8.3. Workstations

### 8.3.1. System Overview

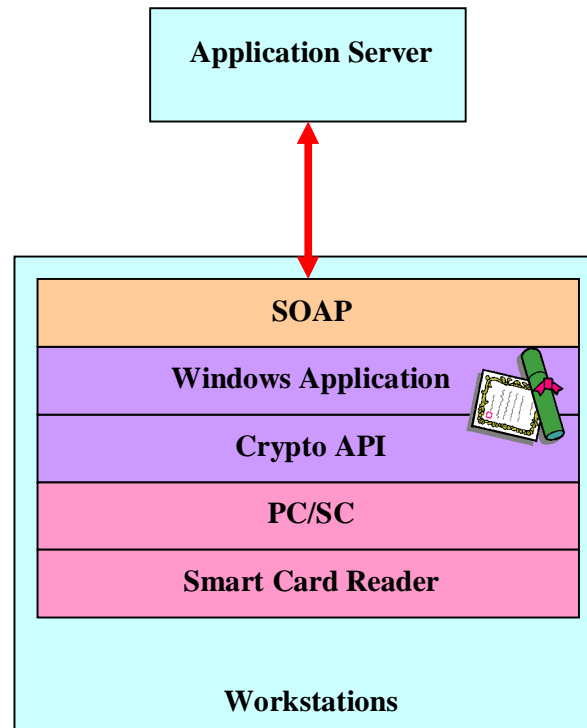


Figure 16 Workstation Overview

User of Horse Racing System can access resource on their workstations. To guarantee privacy, data integrity, mutual authentication and non-repudiation, PKI technology is applied to establish a secure channel.

### 8.3.2. System Requirement

Workstation is designed to run on Windows system. It is recommended to run on Windows 2000 service pack 4 or later. A smart card reader is needed for reader the Smart HKID card. Several software are required before running application. They are as following:

- 1.) e-Cert Control Manager (Can be download from HongKongPost web site)
- 2.) Internet Explorer 5.5 (IE 5.0 does not support 3 Des)
- 3.) Microsoft SOAP Toolkit

### 8.3.3. e-Cert Control Manager

e-Cert Control Manager (Shown in Figure 17, Figure 18) is a free software provided by Hongkong Post. Customer. It can be download free from Hongkong Post web site. ([http://www.hongkongpost.gov.hk/product/download/ctlmgr/step2\\_text.html](http://www.hongkongpost.gov.hk/product/download/ctlmgr/step2_text.html)) After installed e-Cert Control manager, a cryptographic service provider named **TrustedNet Connect 2 Smart Card CSP** is added to system. Application can manage e-Cert through Crypto API by acquiring this provider.

With e-Cert Control Manager, user can view content of e-Cert on Smart ID card, change the Personal Identity Number (PIN) of your e-Cert on Smart ID Card and manage the e-Cert and key(s) on Smart ID card (using Advanced Mode).



Figure 17 eCert Control Manger

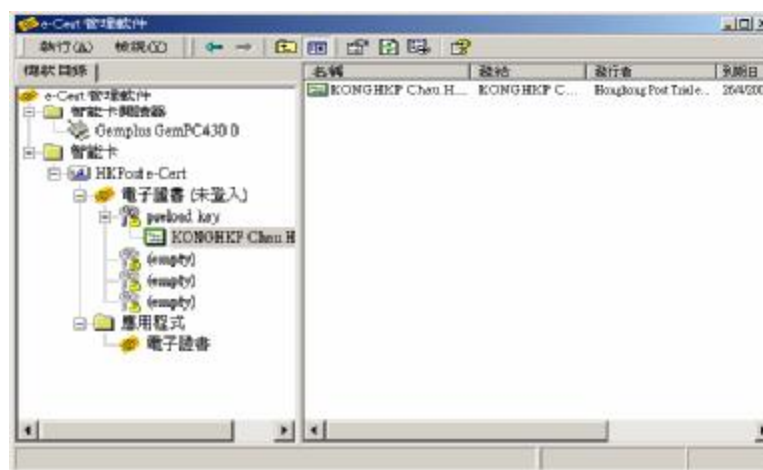
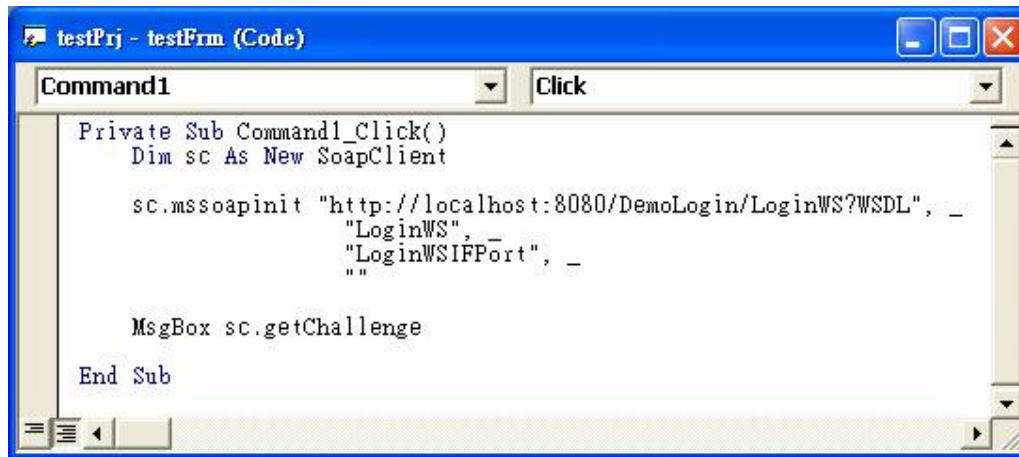


Figure 18 eCert Control Manger (Advance Mode)

### 8.3.4. Microsoft SOAP Toolkit for Web Service Client

Microsoft Visual Studio .NET tools make creating a Web Service surprisingly simple. The MS SOAP Toolkit, even though it is based on COM technologies, also simplifies Web Service creation (Shown in Figure 19). Three lines of source code can initialize a SOAP request. However, there are more things to think about before rolling out your first production Web Services.

The image shows a screenshot of a Visual Studio code editor window titled "testPrj - testFrm (Code)". The window contains a code editor with the following source code:

```
Command1 Click
Private Sub Command1_Click()
    Dim sc As New SoapClient

    sc.mssoapinit "http://localhost:8080/DemoLogin/LoginWS?WSDL", _
        "LoginWS", _
        "LoginWSIFPort", _
        ""

    MsgBox sc.getChallenge
End Sub
```

Figure 19 Source code of sample Web Service client program

**The trick to thoughtful implementation of security measures is to strike a balance between securing the system and making it easy and useful for end users.**

*Building an Extranet; Julie Bort, Bradley Felix ; John Wiley & Sons, Inc., 1997*

### 8.3.5. Windows Application

Windows application *Horse Racing Client* provides GUI for customer to view their account information and betting. Customer has to login and finish Mutual Authentication before submitting any instruction. The required certificate chain for authenticating server has been embedded into *Horse Racing Client* during installation.

Horse Racing Client provides four functions. They are login, view balance, bet and logout. Customer has to installed e-Cert Control Manager and insert Smart ID card into smart card reader before login. All exchanged data will be transfer in 3DES encrypted format.

### 8.3.6. Crypto API

Crypto API is a standard API defined by Microsoft. It is intended for use by Windows application developers. The other open standard method is PKCS11. *Horse Racing Client* will access Smart ID through Crypto API. It is because Crypto API provides flexibilities of switching cryptographic service provider without changing design. The following APIs are exported by library (HRSCryptoLib.dll) which wrapped Crypto API COM.

- 1.) BSTR Base64Encode (PBYTE inArray)
- 2.) PBYTE Base64Decode (BSTR inBstr)
- 3.) PBYTE RSAEncrypt (PBYTE inArray)
- 4.) PBYTE RSADecrypt (PBYTE inArray)
- 5.) PBYTE Envelop (PBYTE inArray)
- 6.) PBYTE Develop (PBYTE inArray)

Other than Crypto API, there are another methods to access the e-Cert embedded in Smart HKID is through PKCS11.

#### PKCS #11 - Cryptographic Token Interface Standard

This standard specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.

## 8.4. Terminals

### 8.4.1. System Overview

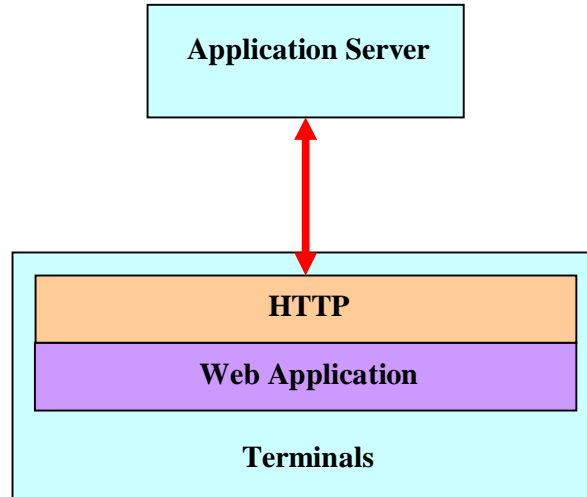


Figure 20 Terminal Overview



Figure 21 Web Application for Horse Racing System

Terminals can access the web application provided by Application Server. This web application provides to Administrator for managing Horse Racing System. The following sections will describe the features of Horse Racing System.

### 8.4.2. System Requirement

Terminal is designed to run on Windows system. It is recommended to run on Windows 2000 service pack 4 or later. No special software is required.

### 8.4.3. Stable Management

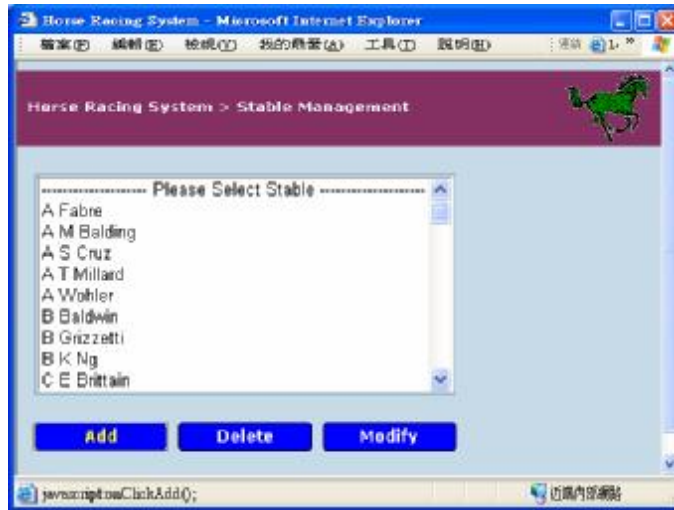


Figure 22 User Interface of Stable Management

This module provides four management functions:

- 1.) Add Stable – Add a new stable to database

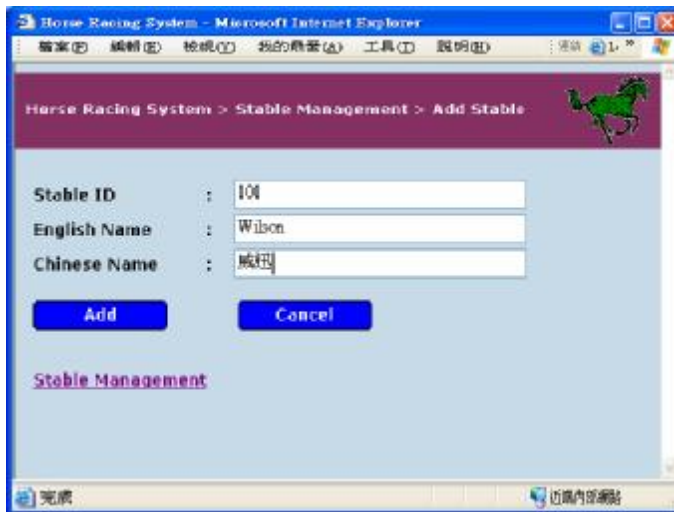


Figure 23 User Interface of Adding a new Stable

2.) Delete Stable – Delete an existing stable from database

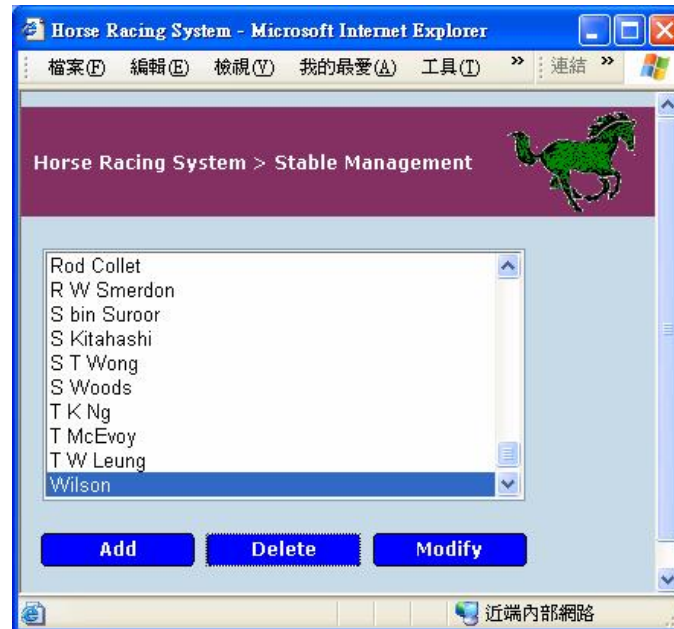


Figure 24 User Interface of Delete a new Stable

3.) Modify Stable – Modify the stable information. Including the related horses, jockeys, trainers and stable owners.

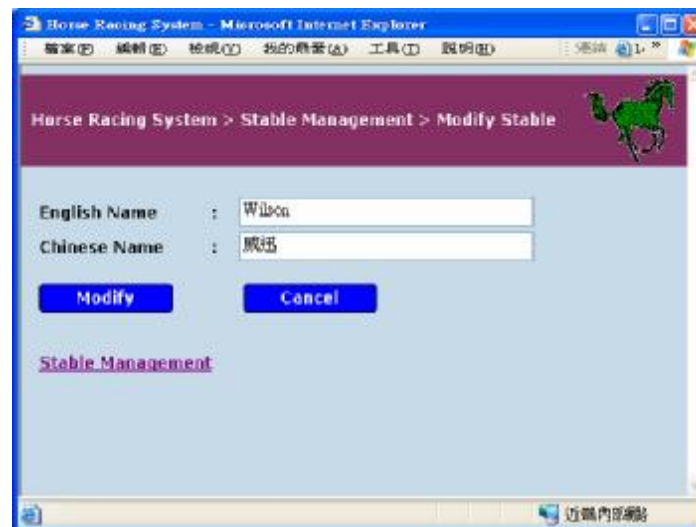


Figure 25 User Interface of Modifying a Stable

4.) Search Stable – Search a stable from database



### 8.4.4. Race Management

This module provides four management functions:

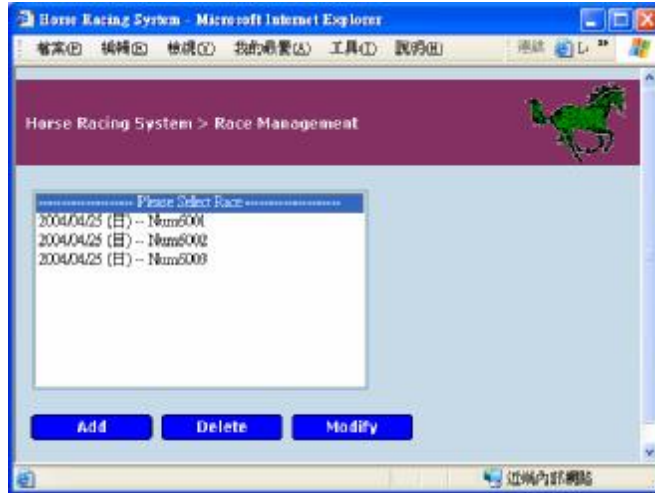


Figure 26 User Interface of Race Management

1.) Add Race – Add a new race to database.



Figure 26 User Interface of Adding a new Race

2.) Delete Race – Delete an existing from database.



Figure 27 User Interface of Deleting a Race

3.) Modify Race – Modify the race information. Including the related horses and Jockey, race status and race result.



Figure 28 User Interface of Modifying a Race

4.) Search Race – Search a race from database

#### **8.4.5. Jockey Management**

This module provides four management functions and the user interface is similar to Stable Management:

- 1.) Add Jockey – Add a new jockey to database.
- 2.) Delete Jockey – Remove an existing jockey from database.
- 3.) Modify Jockey – Modify the jockey information.
- 4.) Search Jockey – Search the jockey from database.

#### **8.4.6. Horse Management**

This module provides four management functions and the user interface is similar to Stable Management:

- 1.) Add Horse – Add a new horse to database
- 2.) Delete Horse – Delete an existing horse from database.
- 3.) Modify Horse – Modify the horse information.
- 4.) Search Horse – Search a horse from database.

#### **8.4.7. Trainer Management**

This module provides four management functions and the user interface is similar to Stable Management:

- 1.) Add Trainer – Add a new trainer to database.
- 2.) Delete Trainer – Delete an existing trainer from database.
- 3.) Modify Trainer – Modify the trainer information.
- 4.) Search Trainer – Search a trainer from database.

#### **8.4.8. Stable Owner Management**

This module provides four management functions and the user interface is similar to Stable Management:

- 1.) Add Stable Owner – Add a new stable owner to database.
- 2.) Delete Stable Owner – Delete an existing stable owner from database.
- 3.) Modify Stable Owner – Modify stable owner information.
- 4.) Search Stable Owner – Search a stable owner from database.

## 8.5. Database Server

### 8.5.1. System Overview

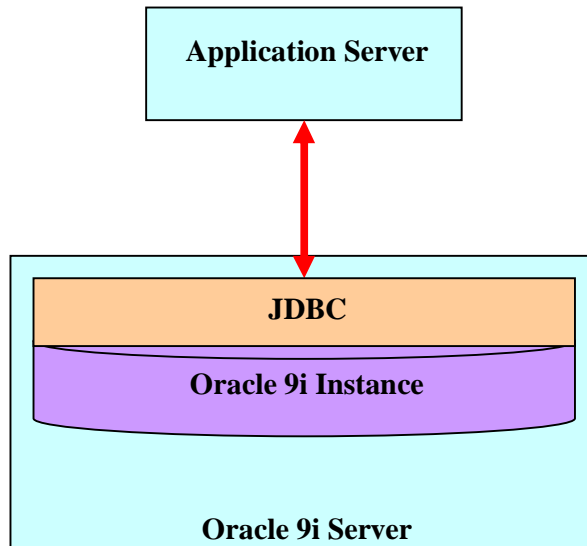


Figure 22 Database Server Overview

High Availability (HA) is becoming a must-have requirement for e-businesses that cannot afford system down time. Oracle Real Application Clusters are the multi-node extension to Oracle database server. They enable e-businesses to build a multi-node database server that are highly available and highly scalable. ORAC architecture makes Oracle cluster databases highly available while functioning as highly scalable database servers. Horse Racing System can be made more available when building a highly available application system. It is proven that Oracle cluster database, with active instances on all nodes, is also a much better choice for database fail-over solution than those offered at operating system level for generic application fail-over. This is a real mission critical solution

#### What is Oracle database failover?

Oracle database files and resources are protected by monitoring key Oracle processes and file systems. When an Oracle database or dependent resources is detected not to respond, LifeKeeper initiates a recovery scenario that attempts recovery on the local server. If this recovery fails, then the database is recovered on the remote server.

The core LifeKeeper product assumes that shared storage will ensure data availability. If no shared storage is available then data availability must be ensured via LifeKeeper Data Replication.

### **8.5.2. System Requirement**

Database server is designed to run on Windows system. It is recommend that the running machine at least have 1G RAM assigned for Oracle. Otherwise, database server performance will be degraded.

## 8.6. UDDI Registry Server

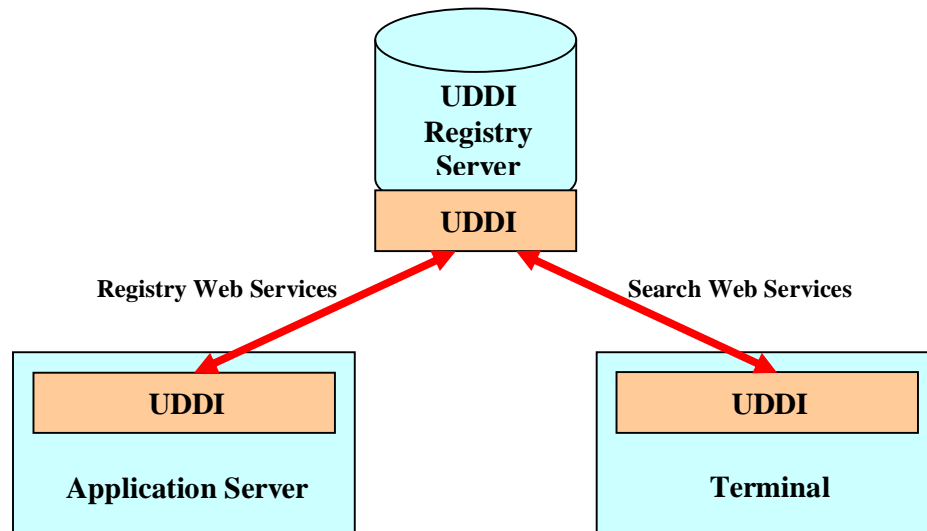


Figure 23 UDDI Registry Server Overview

Universal Description, Discovery, and Integration (UDDI) provides the means for registering and finding information about businesses and the Web services they support. In UDDI Registry Server, information is stored in a registry. A registry is a central database of businesses and Web service specifications.

The information in a UDDI registry is a combination of white pages, yellow pages, and green pages data. These provide business contact information, categorize businesses and services, and provide technical specifications of services, respectively.

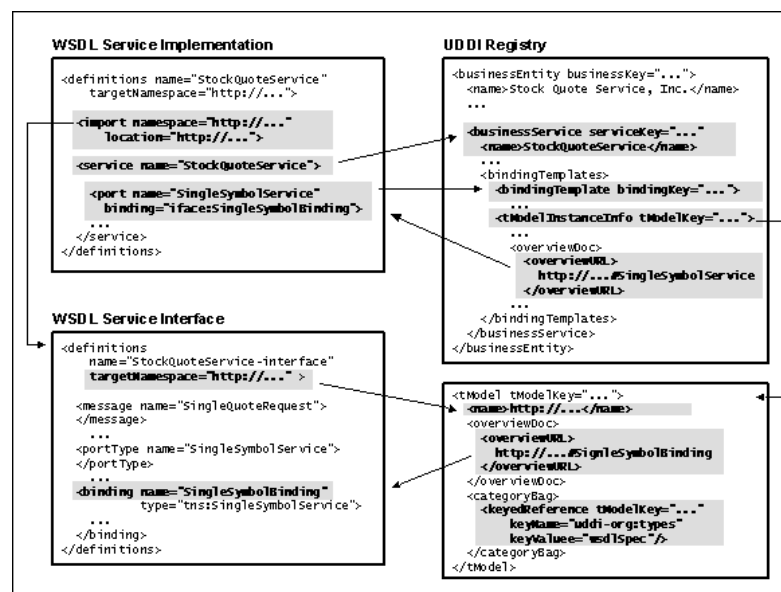


Figure 24 The work flow of Web Service

## **8.7. Firewall**

### **8.7.1. Introduction**

Firewalls were built to stop fires from spreading. It typically guards an internal network against malicious access from the outside and stopped intruders from passing into the network.

### **8.7.2. Software Firewall**

Software firewall differs from vender to vender, but all firewalls have an underlying operating system. This operating system can be used for other services entirely, but it is important to understand that incorporating other services into your firewall will increase the chance of a successful intrusion. It is encouraged to have a standalone machine for firewall duties.

### **8.7.3. Hardware Firewall**

Hardware firewall is generally no different from any other workstation or server except that it has two or more network cards. It is useful to know that a firewall has all the functionality of a network router (it routes data as well as filtering it) and can therefore replace an expensive router if needed.

### **8.7.4. Zone Alarm**

Zone Alarm is a free product of Zone Labs. It is a software firewall with configurable control list for Windows Service. In Horse Racing System, Zone Alarm will act as a firewall and block all network traffic except HTTP. This approach will further enhance the security level of Horse Racing System.



### 8.8. Database Scheme

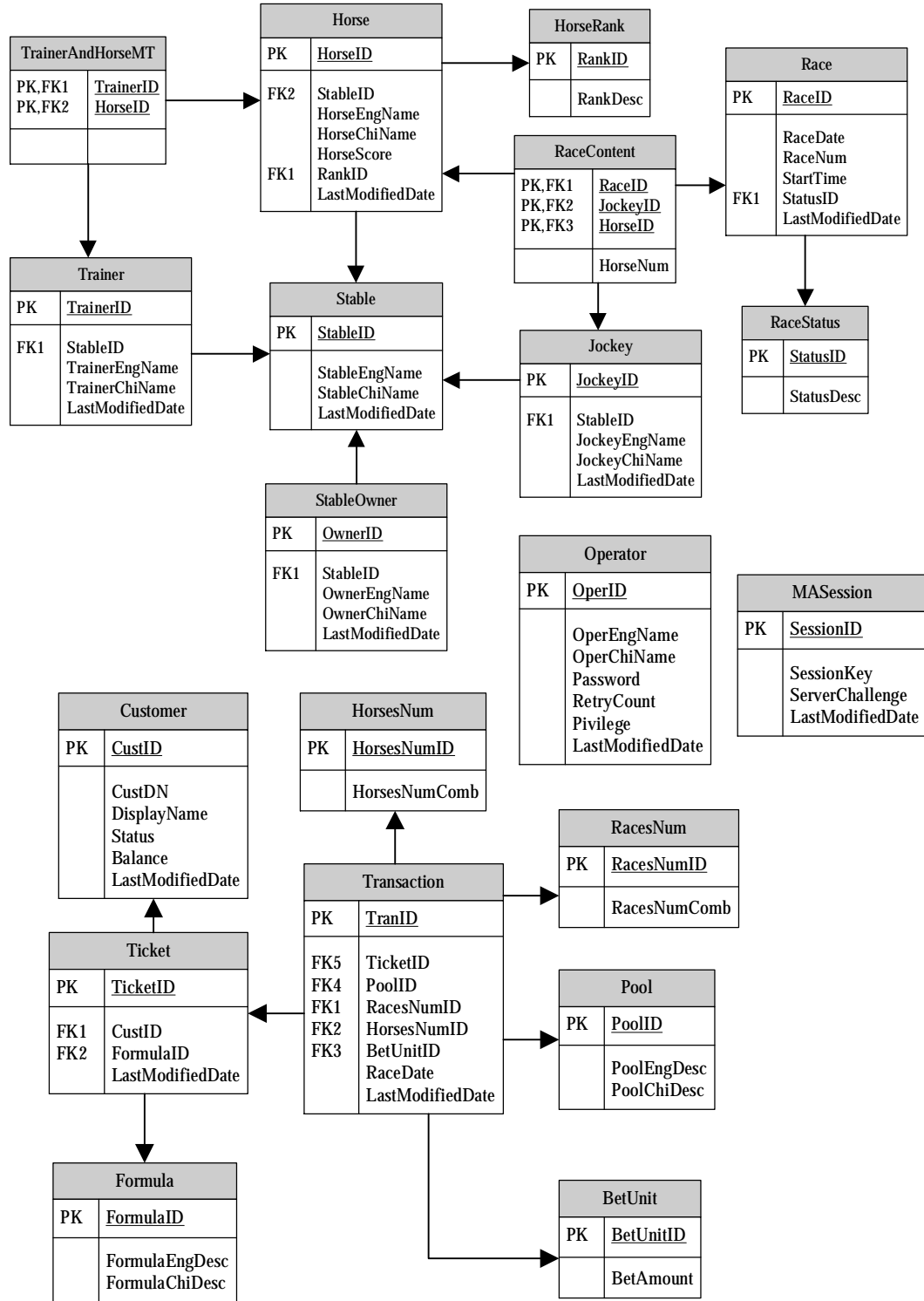


Figure 25 Schema of Horse Racing System



### 8.8.1. Code Table

In order to reduce the complexity of database scheme, several code tables have been created and simplify the programming logic. Each code table contains a static list of entries which is not likely to be change. They are

1.) RaceStatus

Each RaceStatusID stands for race status with Chinese and English description.

2.) RacesNum

This table lists out the possible combination of race number for each transaction. Base on game rules, each transaction bet up to 6 races and 10 races per day. That means the total possible outcomes are  $10nCr1 + 10nCr2 + 10nCr3 + 10nCr4 + 10nCr5 + 10nCr6$ .

3.) HorsesNum

This table lists out the possible combination of horse number for each transaction. Base on game rules, each transaction bet up to 3 races and 14 horses per race. That means the total possible outcomes are  $14nCr1 + 14nCr2 + 14nCr3$ .

4.) Pool

Eleven types of Pool are available for betting. Details please refer to [http://www.hongkongjockeyclub.com/english/betting/guide\\_qualifications.htm](http://www.hongkongjockeyclub.com/english/betting/guide_qualifications.htm)

5.) BetUnit

17 types of Bet Unit are available for betting. The valid Bet Unit range will depends on the Pool.

6.) BetFormula

40 types of formula are available for filling ticket. Each formula can create a or more transaction for each ticket.

For the details of code table, please refer to Section 9 Appendix.

### 8.8.2. Mapping Table

Figure 6 and Figure 7 show several object has 1 to many or many to many relationship. In order to save their relationship effectively, four mapping tables are created. They are

- Y TrainerAndHorseMT
- Y RaceContent
- Y CustomerAndTicketMT
- Y TicketAndTranMT

For the details of object relationship, please refers to next topic (Section 8.9 UML Diagram).

## 8.9. UML Diagram

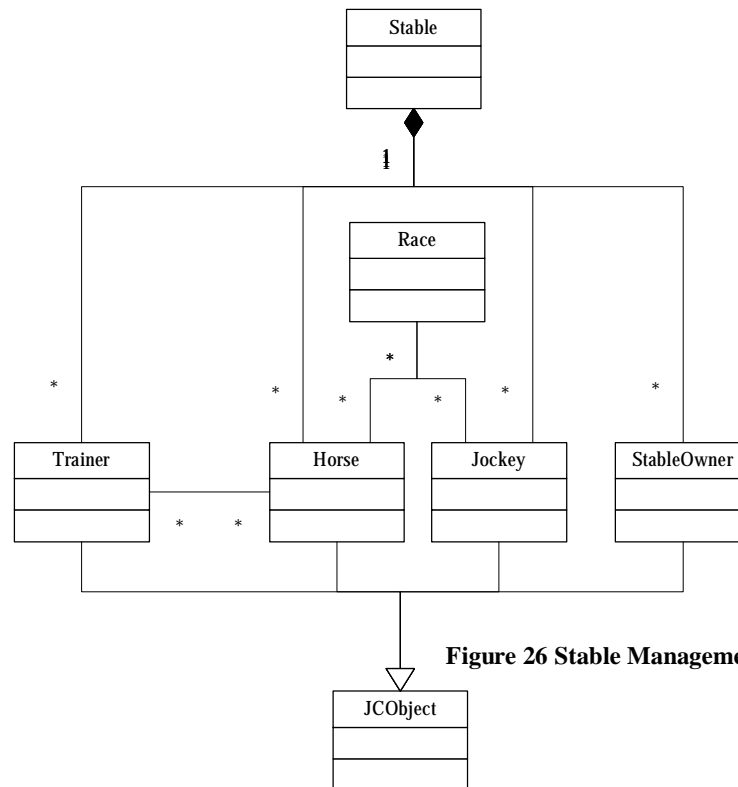
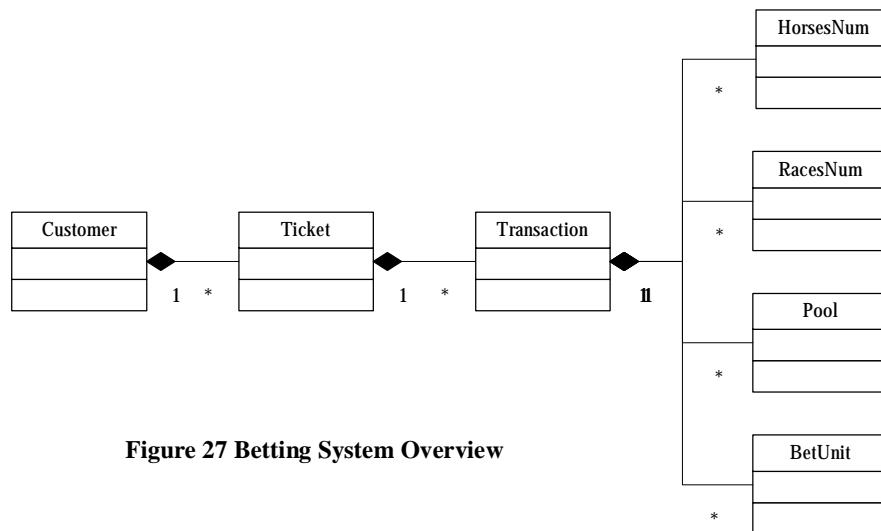


Figure 26 Stable Management System Overview

We can derive stable management object relationships from Figure 26:

1. A Stable has many Trainers, Horses, Jockeys and Stable Owner.
2. A Trainer serves a Stable and trains many Horses.
3. A Horse belongs to a Stable and can be trained by many Trainers.
4. A Stable Owner has a Stable.
5. A Race has many pairs of Horse and Jockey.
6. Trainer, Horse, Jockey and Stable Owner have common characteristics and can be derived from JCOBJECT.



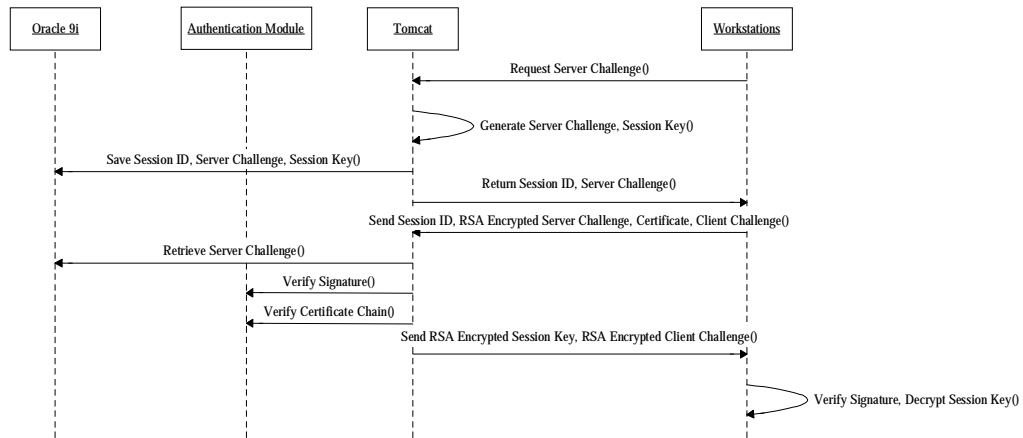
**Figure 27 Betting System Overview**

We can derive betting system objects relationships from Figure 27:

1. Each Customer has many Tickets.
2. Each Ticket represents many Transitions.
3. Each Transaction involves Set of Horse Number, Set of Races Number, Pool and Bet Unit.
4. Set of Races Number is a finite set which define in Section 9.1 CodeTable of RacesNum.
5. Set of Horse Number is a finite set which defined in Section 9.2 Code Table of HorsesNum.
6. Set of Pool is a finite set which defined in Section 9.3 Code Table of Pool.
7. Set of Bet Unit is a finite set which defined in Section 9.4 Code Table of BetUnit.

## 8.10. Workflow

### 8.10.1. Mutual Authentication



**Figure 28 Flow Chat of Mutual Authentication**

Mutual Authentication protects system from middle-man-attack.

- 1.) Client on workstation send a challenge request to server
- 2.) Server generates a challenge and saves to Database along with session ID.
- 3.) Return challenge with session ID.
- 4.) Client sign the challenge and send back to server along with session ID, certificate.
- 5.) Client will also generate a challenge and send to server.
- 6.) Server receive signature on server challenge and verify against with database copy.
- 7.) After verify successfully, server sign the client challenge and send back to client with encrypted session key.

### 8.10.2. Secure Data Exchange

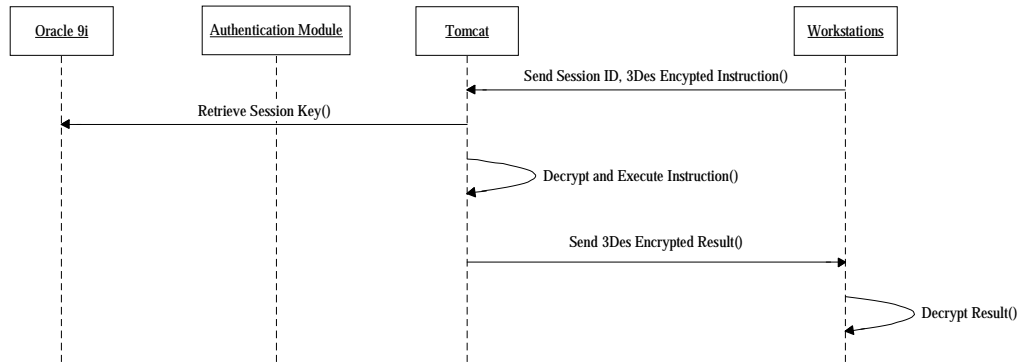


Figure 29 Flow Chat of Secure Data Exchange

To protect data privacy and integrity

- 1.) Workstation send 3DES encrypted instruction with checksum to server
- 2.) Server retrieve corresponding session key. Decrypt instruction and validate the integrity.
- 3.) Proceed the instruction
- 4.) Send 3DES encrypted result to workstation.

### 8.10.3. Session Clean Up

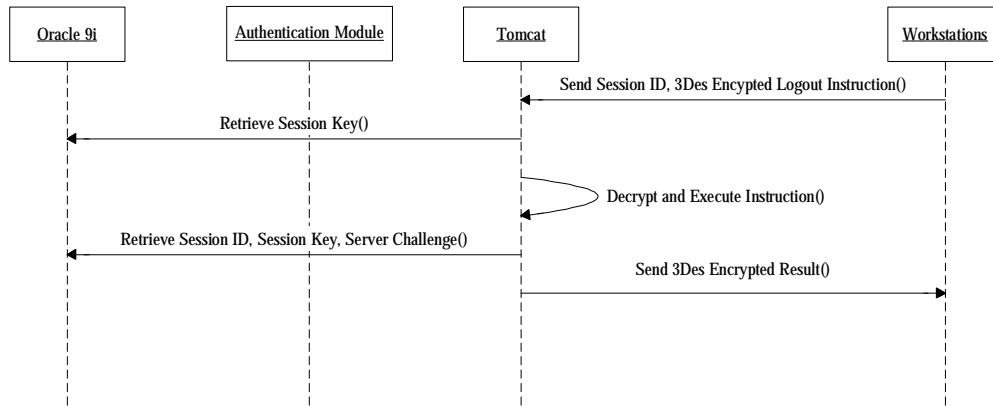


Figure 30 Flow Chat of Session Clean Up

To maintain the cleanness of database, session clean up is require.

- 1.) Client sends logout instruction to server.
- 2.) Server retrieve session key from database. Decrypt instruction and validate the integrity.
- 3.) Remove Mutual Authentication session from database.
- 4.) Send 3DES encrypted result to workstation.

## 9. Appendix

### 9.1. Code Table of RacesNum

(Please see file Appendix I)

### 9.2. Code Table of HorsesNum

(Please see file Appendix II)

### 9.3. Code Table of Pool

PoolID	PoolEngDesc	PoolChiDesc
1	Win	獨贏
2	Place	位置
3	Quinella	連贏
4	Quinella Place	位置 Q
5	Tierce	三重彩
6	Trio	單 T
7	Double Trio	孖 T
8	Triple Trio	三 T
9	Double	孖寶
10	Treble	三寶
11	Six Up	六環彩

### 9.4. Code Table of Formula

FormulaID	FormulaEngDesc	FormulaChiDesc
1	2x1	2x1
2	2x3	2x3
3	3x1	3x1
4	3x3	3x3
5	3x4	3x4
6	3x6	3x6
7	3x7	3x7
8	Single	單式
9	Multiple	複式
10	Banker	單式馬胆
11	Banker Multiple	複式馬胆
12	Multi-Banker	指定位置馬胆

---

**9.5. Code Table of BetUnit**

BetUnitID	BetUnitDesc
1	2
2	3
3	4
4	5
5	10
6	20
7	50
8	100
9	200
10	500
11	1000
12	2000
13	5000
14	10000
15	20000
16	40000
17	50000



## **10. Reference**

Shon Harris, Mike Meyers' CISSP(R) Certification Passport, McGraw-Hill Osborne Media; 1st edition (October 17, 2002)

Ronald L. Krutz , Russell Dean Vines and Edward M. Stroz , The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons; 1 edition (August 24, 2001)

Banking and Finance on the Internet; Mary J. Cronin ; John Wiley & Sons, Inc., 1997

Web Commerce; Kate Maddox, Dana Blankenhorn ; John Wiley & Sons, Inc., 1998

Cybercorp; James Martin ; Amacom, 1996

Building an Extranet; Julie Bort, Bradley Felix ; John Wiley & Sons, Inc., 1997

Net Profit; Peter S. Cohan ; Jossey-Bass, 1999