ABSTRACT
This paper describes an integrated security administration for global organizations and electronic government systems. It integrates certification systems, authorization systems, registration systems and smart card systems. Many organizations today are having departments all over the world. Employees, employers and customers have to access information located in different countries. This complicates management of security systems for the organizations. The challenges that the organization face include providing authentication, authorization, protection of information, non-repudiation, integrity, privacy and other security services in the global environment. Today, organizations usually install certification, authorization, smart card, and registration systems and apply them separately without sharing common data and without any common security administration procedures. Thus, a new employee or citizen, who needs registration services, a smart card, a public key certificate, and authorization attributes must usually identify her multiple times and must perform registration procedure at four different administration stations. In this research, we designed an integrated security administration procedure for all four-security systems, where we register users only once and the four security systems share all relevant security data and procedures. Therefore, the new integrated security administration is more efficient than existing procedures and it is simpler to manage and saves administration costs. This system bases on the Security Assertion Markup Language (SAML). SAML is an XML-based framework for exchanging security information. The research has achieved two goals: functional integration of data and security administration procedures and visual integration through a common security administration interface. These results are of high interest and importance when managing different components of an integrated security system.

KEYWORDS
PKI System, authorization, SAML, Directory system, smart card system, certification authority and attribute authority.

1 INTRODUCTION
The goal of this paper is to describe a generic management security system for open environments. This system is also suitable for governments that are transforming manual government services into electronic services. The system also
applies to organizations that are supplying services to global markets. The government and organizations have to identify customers, employees, employers, citizens in global environments. This management system bases on the Security Assertion Markup Language (SAML) [10]. SAML is an XML-based framework for exchanging security information.

**ORGANIZATION OF SECTIONS**

Section two covers related work and section three discusses Integration. Section four describes the prototype of the system. Section five briefly discusses conclusions.

2 RELATED WORK

2.1 SMART CARD SYSTEM

Today smart card systems are managed in the following way [1]. The system consists of a central card management component, a card-personalizing component, a printer, an integrator, an enrolment component, a cardholder database, a logical access control component, a physical access control component and a certification authority server. At an enrolment component, a cardholder registers her information. With the help of a digital camera, a normal scanner, a biometric scanner and other equipments, cardholder’s photograph, signature and other data enter the enrolment component.

The enrolment component sends information to an integrator. The integrator takes physical and logical privileges from the physical and logical access control components respectively, and combines them with the data from the enrolment component. The integrator sends this information to the card management system. This is responsible for updating the cardholder’s database. The database stores information about expired, lost, and stolen smart cards, copies of the cardholder’s information, etc. This component takes cardholder’s certificate, data from the card management system, and other data and personalizes the card. The system prints and issues the smart card to a cardholder.

2.2 ROLE–BASED ACCESS CONTROL (RBAC) SYSTEM FOR SECURING A WEB-BASED WORKFLOW

Ahn, Sandhu, Kang and Park [3] describe a way to add a RBAC system to an existing web-based workflow system. A web-based workflow system consists of an interface for clients, a gateway to external services, a tool for protocols, and workflow tool for descriptions and enforcements, where the workflow performs activities in coordination. Different servers execute different tasks. These systems provide only low-level security services such as simple authentication. Authentication and authorization security services bases on public key certificates. The system uses HTTP protocol for client–to–server communication and uses CORBA’s network addressing protocol for server-to-server communication. The system attaches different roles to each task. The system verifies users’ identities and checks whether authorized to perform tasks, which they desire. The Role–Based Access Control (RBAC) model in this system has a set of roles, a set of permissions and users. This model supports role hierarchies. The system assigns permissions to roles and users have different roles. Users can have one or more roles. A role can be assigned one or more permissions and vice versa.

The system consists of three major components: a workflow design tool, a role server, and a web-based workflow system. The administration of the system applies the workflow design tool for generating roles; building role hierarchies; assigning roles to tasks, specifying flows of information and relationships among tasks and for passing information to the role
server. The role server has two components: a user-role assignment component and a certification server. The functions of user-role component include assigning users to roles, and creating and managing role hierarchies and databases. The certification server is responsible for verifying users’ identities, fetching users’ information from databases, and issuing certificates with users’ role information. The workflow system contains web-based task servers. A task server approves authorization to a client based on the information found in user’s certificate. The client is given authorization during the establishment of an SSL [7] session between a client and a task server. The Web server asks for a client certificate during SSL handshaking procedures. Client sends a certificate to the server. The server verifies the identity of the client. The server extracts authorization information from the client’s certificate and checks whether to authorize the client.

The advantage of this system is that the administrator needs to make very little changes on the server side and no changes on the browser’s side. If one web server is compromised, it does not cause the system to stop, because servers are doing multiple and different tasks. The disadvantage of this system is that both authentication and authorization information are stored in public key certificates. Different authorities could set and update authorization and authentication information. It is also inconvenient because different authorities can have different policies. Validity of authorization information and authentication can also be different.

3 INTEGRATION
This section describes integration of security management functions and procedures of the directory system, PKI system, smart cards system, and authorization system.

3.1 METHODOLOGY
The procedures of the components were analyzed first. Procedures were analyzed to determine which of them were common in all the systems and the result is shown in Table 10.

Security management procedures of the directory, PKI, smart card, and authorization systems are integrated in such a way that an administrator does not need to perform the same action four times for each individual security system as indicated in table 10.

Registrations of users, identification of users, and verification of users’ identities are performed once for each user. Data are then shared by individual security systems and are available to each of these systems. When a public certificate is issued, it is stored in user’s smart card, in the directory system, and in the certification authority’s database at the same time. When authorization attributes are issued to a user, they are stored in user’s smart card, in directory system, and in authorization system at the same time. All shared data and procedures are integrated through a single graphical user interface, available to the security administrator. Data and procedures are displayed and available in a user-friendly form. The administrator can view data belonging to individual security systems and may register and update entries from the same interface.

3.2 DESIGN OF THE SYSTEM
The directory, X.500 [2], Public key Infrastructure (PKI), authorization, and smart card systems provide the basic ISO security services: authentication, access control, data confidentiality, data integrity, and non-repudiation. The security platform, that contains libraries and security mechanisms, supports this system. We
apply the Lightweight Directory Access Protocol (LDAP) [4] for accessing the X.500 directory. LDAP has methods and interfaces for communicating with the X.500 directory but these interfaces are not object-oriented and are very complicated for a normal user. In this work, we have created generic objects and object-based interfaces to solve the problem. We have developed a single PKI system [5] and it has objects and interfaces for certification, registration of users and organizations, management of certificates and keys, etc. The authorization system bases on the SAML [10]. The smart card system has objects and interfaces for formatting smart cards, creating file systems, for initialization, personalization of smart cards and other management procedures. We implement the US Government Smart Cards Architecture standard [8] in this research.
### TABLE 10: ANALYSIS OF PROCEDURES

<table>
<thead>
<tr>
<th>Function</th>
<th>Smart cards</th>
<th>Directory</th>
<th>Authorization</th>
<th>PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration of Users</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Issuing Certificates (PKI, AC)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Creating a CRL</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Publishing Certificates</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Verification of users’ ID &amp; Data</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Storing Certificates</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Validation of Certificates’ Chains</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cross-certification</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Updating objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Submitting CRL</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Initialization of Cards</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Personalization of Cards</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Issuing Smart Cards</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Revoking objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SC Backups</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stolen and Revoked SC</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Protection of objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Creating Roles</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Delete Object</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Setting ACL</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Loading Applets</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Display object</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Adding objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Recovery Operations</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

![Security Assertion Markup Language Diagram](image)

**FIGURE 31: SECURITY ASSERTION MARKUP LANGUAGE**

Figure 31 shows the integrated system. A company for example can have integrated security systems in different departments, which could be located in different cities and different countries. Secure Multiple Internet Extension (SMIME) [9] and Public
Key Cryptographic Standard (PKCS) [10] will protect communication among these departments.

3.3 THE GENERAL MODEL OF THE SYSTEM

The system comprises the PKI system, the Authorization system, the Smart card system, a Policy decision point, the Directory system, the SAML [10], a client, and a web server as shown in Figure 3. SAML authorities as described in section 2.8 make SAML assertions. In this research, SAML authorities are PKI system, Authorization system, Smart card system, and Policy decision point. One administrator performs authentication, attribute, and authorization decision assertions. The web server has a policy decision point and a policy enforcement point.

3.4 REGISTRATION OF DIRECTORY OBJECTS FROM ONE INTERFACE

Representations from organizations, organizational units, countries, users, servers and other directory objects present their identities and other registration data to the administrator. The system sends applications for registration in the directory to the administrator. Public keys of the applying entities are included in the application forms. The system exchanges session keys for securing communication between them. The administrator of the directory sends to the applying entity a registration form and the public key of the directory. On the registration form, the user can indicate whether she desires to acquire a smart card, and/or certificate and/or an authorization attributes. The user may indicate whether she can personalize a smart card. The administrator of the system verifies the identity of the user the other registration data. If verification is successful, the administrator registers and writes the data into the directory system, into the smart cards system, into the PKI system, and into the authorization system at the same time. Policies are stored in the directory system. The IETF’s [12] Policy Framework working Group is working on a model to represent policy information in the directories [11]. We describe the certification of entities in the following section.

3.5 CERTIFICATION OF CLIENTS

In this work, we are using a single PKI system. There is a top certification authority (TCA), a policy certification authority (PCA), a hierarchy certification authority (HCA) and a local certification authority (LCA). A client sends a certificate request to the LCA. The request includes among others a public key of the client. The administrator extracts data of this client from the directory system. The system processes and issues a certificate to the client. When the system issues the certificate, it stores it in the directory system, in the smart cards system, and in the authorization system at the same time. We apply certain extensions of a certificate that in this research. One such extension is Authority Information Access. We apply this extension to store an IP number of the directory that contains the certificate of the issuer. Another useful extension is CRL Distribution Points, which stores the IP number of the directory that contains the certificates’ revocation list.

3.6 SMART CARD SYSTEM’S ADMINISTRATION

The system performs the following steps in smart system’s administration: Creation of a file system, initialization of the smart card and personalization of the smart card to a specific owner.
3.6.1 CREATION OF FILE SYSTEM OF THE SMART CARD

An administrator starts by creating the directories in the smart card in accordance with the standard used. In this research, we are using the US Government Smart Cards Architecture standard [8] and it has one directory, called Government Smart card Architecture (GSA). Then the administrator creates files in accordance with the standard that the system implements. The US Government Smart Cards Architecture standard has the following files: card capability, general information, card information, personal protected information, access control, login information file, biometrics – X.509 certificate and PKI – Digital signature certificate.

3.6.2 INITIALIZATION OF THE SMART CARD

In this process, the administrator extracts data of the smart card issuer from the directory. The system writes these data into the user’s smart card in a file that contains issuer’s data. In the US Government Smart Cards Architecture standard, the files are card information and general information. The system writes all of the card information file into the card during this process. In the general information file, we write the following fields into the card during the initialization process: organization, organizational unit, department number, department code, postal address, street address, physical delivery office number, locality, state or province, postal code, country and non-government agency.

3.6.3 PERSONALIZATION OF THE SMART CARD

The system extracts user’s data from the directory. The issuer or the cardholder may perform this process depending on the policy of the card issuer. The cardholder may update some or all personal data, while the administrator of the issuing organization updates some data, depending on the policy of the card issuing organization. The system writes data related to the cardholder into the smart card. In accordance to the US Government Smart Cards Architecture standard, we write data to the following smart card files: general information, protected personal information, Access control, Login information, Biometrics-X.509 certificate, and PKI – Digital signature certificate.

3.7 AUTHORIZATION SYSTEM

An administrator starts processing attributes of client by extracting client’s data from the directory. Thereafter an administrator extracts authentication information from the directory. In this research, the system uses a public key certificate of the client for authentication. After successfully authenticating the client, the administrator of the authorization system writes authorization information to the directory. The serial number of the public key certificate is part of this information. This serial number links the certificate to the authentication information to the authorization information. Authorization information can be stored in an attribute certificate or in attributes assertion.

3.8 SECURITY ASSERTION MARKUP LANGUAGE (SAML)

SAML [6] is a flexible Extended Markup Language (XML) based framework for exchanging security information about users on the Internet. SAML supports single sign on, which enables users to visit different sites without needing to login every time. The system represents the
security information in forms of assertions about subjects. Assertions contain authentication information, attributes of subjects and information about authorization decisions on resources. The SAML authorities manage and issue assertions, which include authentication authorities, attributes authorities, and policy decision points. Clients can request for assertions from the SAML authorities. Requests and responses are in the XML [15] formats. The protocol used for carrying the requests and responses is the Simple Object Access Protocol (SOAP) [14] over HTTP. SOAP bases on an XML based protocol and exchanges information in open environments. An assertion contains the following elements; major version, minor version, assertion ID, issuer, issuer’s instant, conditions, advice, XML signature [13], statement, subject statement, authentication statement, authorization decision statement and an attribute statement. The SAML architecture has the following components: a credentials’ collector, an authentication authority, an attribute authority, a policy decision point, a system entity (subject) and a policy enforcement point. The authentication authority, attribute authority, and policy decision points make decisions basing on policies. In this work, the PKI is an authentication authority, and authorization system is an authorization authority. A system entity logs in a domain and the authenticating authority authenticates the entity basing on the credentials supplied. The result of this process is stored in an authentication assertion as shown in Figure 31. The system creates a reference to this assertion, it is in the form of a ticket, and sends it to the entity. The entity can supply this ticket to different websites and will be authenticated basing on the ticket. If a website needs authorization information, the website contacts the attribute authority and requests for an attribute assertion. The system sends this assertion to the policy decision point, which issues the authorization decision assertion. The system then sends this assertion to the policy enforcement point on the website. The website will grant access to the requested resources depending on the authorization decision assertion.

4 PROTOTYPE

We have partly implemented this system and we briefly describe the prototype this section. The administrator starts by login into the security management system.

4.1 THE DIRECTORY SYSTEM

The administrator registers an organization, an organizational unit, or a user by selecting the directory from the interface. Then the administrator selects option Registration on the drop-down menu and then option register, then option organization, organizational unit, country or user on the interface shown in Figure 31. We fill the data into the registration forms and write these data into all the components of the system. When searching and retrieving data, the administrator selects the directory to search or retrieve data. Then an entity, organization, country, organizational unit, or user, is selected from which to search or retrieve data and the administrator enters the search string. The administrator updates information in the components by selecting option organization, organizational unit, country, or user and then selecting update from the menu. The update action enables data to be modified in all the components of the integrated system.
4.2 THE PKI SYSTEM
An employee or customer of an organization sends a certificate request to the administrator of the system. The administrator processes the certificate request by selecting Local CA from the PKI system in the interface, then organization and then certification. The administrator approves the certificate request of the organization by selecting certify and then choosing the request to be processed from the list of certificates’ requests. The certificate is then issued by selecting issue certificate in the menu. A certificate of a user is created in the same way as that of an organization. The issued certificate is then stored in the user’s smart card and in the directory system. To revoke a certificate an administrator selects option Certificate and then revoke and the certificate to be revoked. The administrator can perform other management actions like list certificate, delete certificate and so on.

4.3 SMART CARDS SYSTEM
An administrator creates the file system of the smart card. Then the administrator performs login session as shown in Figure 32 and then chooses option Smart Card from the drop-down menu and creates the file system by selecting Initialize Card. The first time this option is selected it activates creation of a file system of the smart cards, while the second selection causes initial data to be written to the smart card.

4.3.1 INITIALIZATION OF THE SMART CARD
An administrator selects smart cards system from the interface. Then the administrator selects option Initialize Card from the drop-down menu in the interface. In this process, the data related to the issuer of the smart card are written to the user’s smart card. Issuer related data are extracted from the directory system.

4.3.2 PERSONALIZATION OF THE SMART CARD
An administrator selects smart cards system, then option Smart Card and then option Personalize Card from the drop-down menu. In this process the personal data specific to the cardholder are written to the smart card. Personal data of the cardholder are extracted from the directory system.
5 CONCLUSIONS

This research has achieved integration of diversified security administration procedures through functional and visual integration. As a result, the integrated security administration system specified in this research simplifies user and administrator’s procedures. The user now goes to one administrator instead four different administrators. The system also simplifies activities of an administrator because she now performs administration from one interface on one machine. The administrator performs user’s registration once and data is shared by all the subsystems. From one machine, an administrator is able to visualize the whole system with all the components. The system reduces administration costs. The system uses SAML, an XML based framework, for exchanging security information between clients and web servers. This simplifies transfer of information because in one assertion we can have information about authentication of subjects, attributes of subjects and authorization decisions on resources.

It is expected that contributions and benefits of this research are the following:
- Easier administration of security system components;
- Easier reconfigurations, additions, and upgrades of the security system; and
- It is a flexible system and it is easier to extend with other components. A new component can be integrated with this system by performing an analysis of functions and data in the new component and then integrating the functions and data of the new component with the existing integrated system.

SAML is a flexible framework for exchanging security information and facilitates integration among different security components. Reduction of administration costs

Future work can include further extensions to the system to add notary system, trusted third party time-stamping system and to support conflict resolution services.
ACKNOWLEDGEMENT
Dr. Kasun De Zoysa, now at the Colombo University, Sri Lanka, for creating the security platform and for many advices
Chen Chen, at Computer Science Department, The George Washington University, Washington DC, USA, for participating actively in the development of the prototype.

REFERENCES