2012 Tenth International Conference on ICT and Knowledge Engineering

Enhancement of Security in the Hierarchy Model of Control and Automation by Applying Single Sign-On Approach for Web Services

Peyman Jafary, Andrei Lobov, Jose L. Martinez Lastra
Department of Production Engineering
Tampere University of Technology
Tampere - FINLAND
Peyman.Jafary@tut.fi, Andrei.Lobov@tut.fi, Jose.Lastra@tut.fi

***Abstract*—Information security is an important term in both fields of IT systems and control systems. Thus, security requirements should be always considered in design phase. Modern approaches in manufacturing and automation technology such as: DPWS and OPC UA tend to integrate control system networks to the computer networks by the aid of service-oriented architecture technology. Single Sign-On is a property of access control in information security which focuses on authentication mechanism. It can be performed across federated domains and provides a single entry point for the user that can login only once and become capable of accessing to disparate protected resources in different locations. The Security Assertion Markup Language (SAML) can be used invisibly in background of system and apply as the standard for providing Single Sign-On mechanism by exchanging identity information to different security domains regardless of the specific authentication protocol which is used for identities in that domain. This paper proposes the model for performing of Single Sign-On approach for protected devices and applications that support web services technology and locate across different boundaries of the hierarchy model of control and automation.**

***Keywords*—authentication, identity federation, hierarchy model of control and automation, saml, security token, single sign-on, soap, web services security**

I. INTRODUCTION

In factory floor, different industrial communication protocols are applied in order to create network between sensors, actuators, transducers and I/O devices which is called Device level network. Moreover, controllers, PC based controllers and HMIs can connect to each other and form a network which is called Control level network. [1] This control level network is connected to the Manufacturing Executing Systems and finally to Enterprise Resource Planning systems in order to manage information across entire organization. Traditional models of manufacturing have designed separate networks for factory floor devices and business systems but nowadays plant-to-enterprise networking approach by the aid of state-of-the-art technologies such as: DPWS [4] and OPC UA is spreading fast and manufacturers are trying to provide connectivity from device level network in plant to enterprise system network in order to achieve the goals of globalization. Modern manufacturing systems require considering of flexibility and adaptability that make them to become more time-driven and time-oriented. [11] Moreover, manufacturing systems need seamless integration of machineries, devices and software tools in order to make their interaction and collaboration more efficient. [12] Web services are being considered as a potential technology in the Internet area which integrates heterogeneous devices and creates cross-layer communication. [13]

Since some password-protected devices in factory floor need to interact with each other as well as secured business applications in enterprise level, sophisticated authentication infrastructure would be required for each identity within the hierarchical model of control and automation system. An important approach in field of authentication of web services is web services Single Sign-On (SSO) which can be an advantageous mechanism in order to lower burden on security administrators and making convenient operation for users. In the following, first survey of security technologies and requirements in different levels of Plant-to-Enterprise framework are explained in the section 2. Then, the proposed architecture model for Single Sign-On (SSO) approach of web services-enabled resources in the hierarchy model of control and automation is discussed in the section 3 and finally conclusion is presented in the section 4.

II. SECURITY IN PLANT-TO-ENTERPRISE FRAMEWORK

Network is an important component in automation and multiple networking layers can be identified by respect to the analogy of ISA95. Automation systems and technologies in various layers are organized hierarchically and form a model which is called hierarchy model of control and automation. In factory environment, new field devices are updated to the standard networking protocols such as: Ethernet and TCP/IP

978-1-4673-2317-8/12/$31.00©2012 IEEE

that provide connectivity of field devices to the Internet. In case of connecting industrial network to the Internet, although it presents some advantages like improvement on economics but on the other hand vulnerability of the system to cyber-attacks will be increased, this becomes more significant for SCADA networks of important industries. So, security plays vital role in industrial networks and should be always considered in factory network administration. Furthermore, varieties of technologies are used for cross-layer communication in the hierarchy model of control and automation. One of them is web service technology which is employed in modern automation technologies such as: DPWS and OPC UA and make them capable of communicating with ERP systems and finally to the Internet. Security requirements should be deployed in protocols and devices which are used for communication between layers. Security standards in field of industrial networking are emerging but in the field of enterprise (IT) networking are contained and comprehensive. Information security attempts to achieve three main goals: Confidentiality, Integrity, and Availability (CIA). In enterprise network, priority of three mentioned aspects is: Confidentiality, Integrity and finally Availability but in industrial automation and control networking priority is opposite of enterprise network i.e. Availability, Integrity and Confidentiality. [1]

A. Industrial Network Security

Although some standards like secFB [14] have proposed for increasing the security of Fieldbus networks but security in Fieldbuses is not as mature as computer networks. The first solution for increasing of security can be implementing of the Internet security protocols to industrial network but unfortunately it is not feasible because most of the internet security protocols operate in top layers (most often layers 3, 4 and 6) of the OSI networking layer model but majority of industrial networks (Fieldbuses) are implemented in layer 1, 2 and 7 of OSI model and they cannot apply security protocols which are used in the top layers of the OSI model. Furthermore, if Internet security protocols apply for industrial network then they cannot support real-time behavior which is one of the main requirements in industrial network. [3] Although, industrial network protocols have so limited complexity in compare with computer networks but two main problems exist for providing security of industrial networks. First, Fieldbuses are based on lightweight communication protocols and do not support built-in security functions and second, most of the existing Fieldbus nodes work with limited processing power and they do not have powerful enough microprocessor for supporting cryptographic operations like encryption. [3]

Cryptographic methods can be utilized for securing of transmitted data in industrial networks. Encryption is a popular cryptographic technique that provides confidentiality for transmitted messages in the network by masking the content of the message. In this technique, content of the messages alter by the help of an encryption algorithm and messages transforms to unreadable data except for who knows the encryption algorithm. The most common encryption technique is symmetric encryption that uses the single secret key for both encryption and decryption of data but the other encryption technique with enhanced level of security is asymmetric encryption that is applied in Public-Key Cryptography system and uses two different secret keys: public key and private key which are used for encryption and decryption respectively.

Another cryptographic technique is called authentication and used for protecting system against alteration of data. By applying authentication to the message, communication parties assure that content of the message has not changed and it came from authentic source. Authentication can be achieved either by use of symmetric encryption or by applying some other methods for message authentication which are not based on encryption technique such as: Message Authentication Code (MAC) and one-way Hash Function. [3]

The Defense-in-depth security model proposes multiple security layers which are considered all over the industrial automation and control networks. The security layers in Defense-in-depth model consist of: Device security, Application security, Computer security, Network security and Physical security and they provide security for data, applications, endpoints, plant and workers. [1]

The network of industrial commands in the area of supervisory control level in the hierarchy model of automation and control is called SCADA network and can connect to the enterprise network either through special gateways or directly by employing of integration technologies like web services. Network administrator should determine proper access control and set security requirement for the SCADA networks, this can be done by using some aspects like cryptography, authentication, intrusion detection system, IT firewall and SCADA firewall. IT firewall prevents unauthorized access to the network by checking source IP, destination IP and TCP destination port number in the exchanged messages. Although this mechanism increases the security of SCADA network but it is not enough since communication messages in SCADA systems have no good granularity and SCADA system cannot be completely protected by IT firewalls. The SCADA network protection is completed by SCADA firewall that not only carries out the protection mechanism of IT firewall but also it inspects data traffic in the upper layer of the OSI model which is usually contained specific application operands such as Modbus-TCP commands. In the other words, it checks the communication protocol in more details and realizes what each data packet does in the protocol. For instance, SCADA firewall is capable of filtering the SCADA network traffic by not only IP and TCP port addresses but also by the type of the Modbus-TCP messages such as: read or write messages.

Intrusion detection system (IDS) is used when SCADA networks are connected to the LAN or Internet for monitoring and analyzing network access pattern. Intrusion detection systems (IDSs) can be classified by their location and source of data to be collected (network-based IDS and host-based IDS), purpose of data analyzing (Signature-based IDS and Anomaly-based IDS) and the response taken to detected intrusions (active-response IDS and passive-response IDS). [2, 17]

As it was described earlier, Fieldbuses are proceeding to connect to the enterprise network and the Internet. In case of connecting through a gateway which converts Fieldbus protocol to the transport format data, a client in the Internet can access to the gateway via firewall. From security point of view, it should include an online and offline sections, security clients and administrators are located in the online part and having capability of secure remote access to the data of factory shop floor over gateway. The offline part contains cryptographic devices such as key distribution center which generate and manage required secret keys for the Fieldbus devices. [3]

Another approach is to connect Fieldbus devices to the enterprise network and subsequently to the Internet without using of gateway by the help of integration technologies such as: service-oriented architecture (SOA) standards. Some security standards such as WS-Security, WS-Trust and WS-Secure Conversation are employed in order to enhance security of communication.

B. Cross-Domain Communication Security

Service-oriented architecture communication is the latest solution to achieve interoperability between resources in different layers in the hierarchy model of control and automation. In service-oriented architecture, each application can call functionality from other application over the network. When the functionality is published over the network then discovery and binding are two other important properties, discovery is ability of finding the functionality and binding is ability of connecting to the functionality. XML is commonly used for interfacing with SOA services. Web services technology that is specific XML-based technology in service-oriented architecture. The main parts in web services architecture are web services provider, web services requester and web service broker which are correspond to published, discovery and binding aspects of SOA. [4]

Two other concepts in web services systems are WSDL and SOAP. There is often a machine-readable description of the operations offered by the service written in the Web Service Description language (WSDL) and the Simple Object Access Protocol (SOAP) message is the communication protocol for exchanging structured information between web services. In the other words, SOAP is a technology that enables web services applications talking to each other over HTTP. One of the advantage of web services is that web services traffic use the HTTP port (port 80) or SSL port (port 443) and it signifies that IT firewalls do not block this traffic and network administrator does not need to open the new port in firewall for web services traffic.

The usage area of service-oriented architecture is popular in enterprise level and increasing in automation systems at device level by applying of Device Profile for Web Services (DPWS) from one hand and OPC UA framework from other hand. [13] In DPWS applications channel-based security is achieved by applying Transport Layer Security (TLS) mechanism for providing encryption and authentication between device and client at transport level. DPWS security at message level is achieved by using of standards such as: XML signature, XML encryption, WS-Security, WS-Trust and WS-Secure conversation.

In order to achieve the full level of security in OPC UA technology, all parts of the automation system that includes OPC UA server, OPC UA client and network between them should be protected. The main essential security objectives are: authentication and authorization (for both user and application), confidentiality, integrity, auditability and availability which are presented in the OPC UA security model that addresses the security functionalities in different layers: application layer, communication layer and transport layer. [18]

By applying of web services standards at device level, heterogeneous Fieldbus devices can be integrated into other layers of the hierarchical model of control and automation and cross-layer communication becomes possible in order to increase responsiveness of factory as a whole but communication security issues become more important. In fact, web services technology presents both security challenge and security threats. The security challenge is for implementing security rules at application layer and the threat is that web services open up a new way of attack because it cannot be protected by common IT firewalls since SOAP is most frequently bound to HTTP and consequently uses web ports for communication and IT firewall is not able to recognize this traffic from HTTP traffic. [15]

C. Deploying Service-Oriented Architecture Security

Several emerging technologies and standards such as: WS-Security, WS-Trust, WS-SecureConversation, WS-SecurityPolicy and SAML address different aspects of the problem of security in web services systems. The most important one is WS-Security which discusses about how to include security token (a token is an XML representation of security information) into header of SOAP messages and how to apply XML security standards such as: XML signature and XML encryption in a part of the SOAP message as well as inside the mentioned security tokens.

There are two main approaches for deploying WS-Security standards: Secure endpoint and web services security proxy. Secure endpoint means security protocols process in both application server and client software while web services security proxy is using of secure gateway between application server and client software in which messages are sent to the proxy and then forwarded. Applying of security proxy is

selected as preferable solution because it separates application and security functionality and it can work transparent of existing systems.

SOAP is generally bound to the HTTP which can use SSL for authentication and encryption but this is not enough to guarantee the required level of security because SSL gives just transport-level security and not application-level security. Although SOAP is mostly bound to HTTP but SOAP is independent of underlying communication layers. In the multihop SOAP messages scenario, different communication technologies can be applied, for example HTTP in the first one and SMTP for the next one and so forth. [15] So, end-to-end security cannot depend on the security technology of particular communication technology.

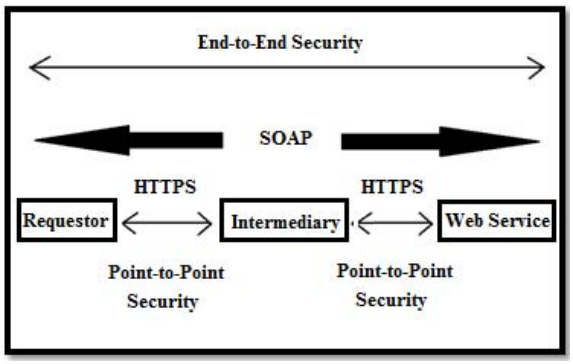

Figure 1: Security and Protocol Layers in Web Services Scenario

In the figure 1, the intermediary element i.e. web service security proxy which is also known as the SOAP firewall checks about the validity of content of SOAP messages at application level. This protection cannot be achieved by using of ordinary IT firewalls which inspect SOAP messages traffic in packet level.

III. SINGLE SIGN-ON APPROACH FOR WEB SERVICES IN THE HIERRACHY MODEL OF CONTROL AND AUTOMATION

As it was discussed earlier, automation devices and applications are located in different domains in the hierarchy model of control and automation. Each domain can be contained protected resources that accesses to them are controlled by specific authentication infrastructure such as: Kerberos or password authentication protocol. In some business processes, user or application in one domain needs repeated access to the secured resource in another domain. In this scenario, user/application must present its security credential which is correspondent to the authentication system of another security domain each and every time the secured resource is invoked and it will be more complicated when authentication protocols in two security domains are different. Single Sign-On mechanism addresses this problem by providing secure and single authentication point for the user/application to authenticate to multiple protected resources in various security domains by entering security credential only one time. Single Sign-On mechanism reduces both operational cost and the required time to access the distributed applications across the hierarchy model of control and automation.

Web services single sign-on can be achieved by applying web services standards such as: WS-Security, WS-Trust, and WS-Federation with proprietary security tokens [16] or by using of SAML token which is the choice in the proposed model in the following. WS-Trust standard provides a standardized interface for issuing, exchanging and validating security tokens as well as managing trust relationship between participants. [5]

WS-Federation describes mechanisms for allowing different security domains to broker security information (identities, attributes and authentication) about identity and security token issuers to services without requiring user intervention unless specified by the underlying policies. It explains about constructing of federated trust scenarios between various Trust domains according to established policies. [6]

The Security Assertion Markup Language (SAML) is an XML-based standard that is capable of presenting framework for exchanging security information (authentication and authorization information) between different partners over the Internet. Since SAML is based on XML which is fully compatible with web services technology, it can be used for exchanging security data about user/application in XML format between security domains irrespective of the applied authentication infrastructure in the security domains. SAML includes several components; an important one is SAML assertion. The SAML assertion which is created by assertion party includes statements about the subject which an asserting party claims to be true. SAML assertions can use with WS-Security that uses SAML assertion as a security token in the header of the SOAP message in order to protect of SOAP messages. The use of SAML assertions with WS-Security is described in the SAML Token Profile. In this case, the assertion which is included in the header of SOAP message would refer to the identity of the requester of message.

Service requester first obtains a SAML assertion from SAML authority by applying of the WS-Trust protocol. A SAML assertion is placed within a SAML token and included in the security element in the header of SOAP message. The key referred to by the SAML assertion is used to construct a digital signature over data in the SOAP message body, signature information is also included in the security header. Service provider verifies the digital signature and uses the information in SAML assertion for security purposes such as authentication and access control. [7]

The proposed architecture model in the figure 2 presents the secure solution for web services Single Sign-On in the hierarchy model of control and automation by using of SAML tokens which are the most widely adopted standard in the industry. [8]

The main aim of the proposed model is that enterprise user takes benefits of single sign-on approach i.e. enter user credential just once and finding access to both protected web services in enterprise zone and cell zone. Protected web service means that user needs to have security information (authentication information) in order to access to them.

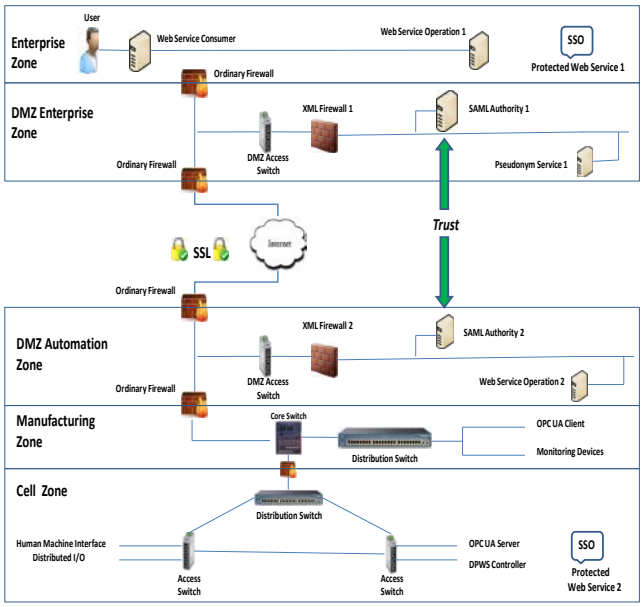

Figure 2: Secure Architecture Model for Web Services Single Sign-On

In this model, there is no direct data traffic between the enterprise and manufacturing zones and all data traffic should originate/terminate in the DMZ zones which provide buffer zones where data and services can be shared between the enterprise, manufacturing and cell zones. In order to keep up the security of system, data management of devices in the Cell zone networks must be performed and controlled through the DMZ Automation zone that allows web services applications in Cell zone network to share data and services with applications in enterprise zone in a secure manner. Security devices such as firewalls are located in DMZ zones. XML firewall is typically deployed behind ordinary IT firewall in order to secure all XML traffic before it reaches the web service on the application server. [1, 9, 10]

Another usage of XML firewall could be apply to create secure federated extranet, where service requestor and service provider locate in various security domains without having any common security policy. This problem can be solved by using of SAML as a common standardized security token to map client-side security policy but the user must have a federated identity. Typically user has local user identity within the security domain of his partner with which he interacts. Identity federation provides a means for these partner services to agree on and establish a common, shared name identifier or identity attribute to refer to the user in order to share information about the user across the organizational boundaries. During account linking process, the local identity of user is linked to the federated identity that will be used to represent the user when the service provider interacts with a partner.

SAML Authority 1 has federated trust relationship with SAML Authority 2 in the other domain. Federation which is the dominant concept in identity management refers to communication of identities between various partner domains by establishing of trust relationship. Federation in different environments will have different configurations based on their needs, security policies, technologies used and existing infrastructure. Pseudonym service which could be either integrated or separated with security token service is applied for federation. Pseudonym is a mechanism which maintains alternate identity information for entities such as clients and services in order to make interoperability with other web services.

The interaction model for web services Single Sign-On in the hierarchy model of control and automation is presented in the figure 3 by respect to the following assumptions that considered being true. First, all service-oriented devices support all required web services standards for single sign-on. Second, SAML 2.0 rules that enhances identity federation capabilities are used in this scenario.

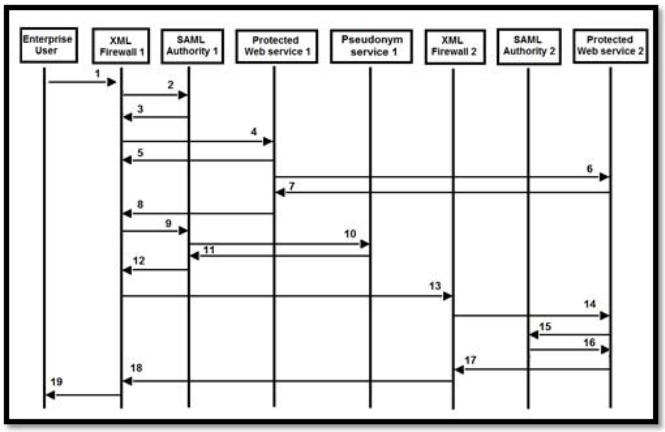

Figure 3: Interaction Model for Web Services Single Sign-On

TABLE 1: DESCRIPTION OF THE STEPS IN THE INTERACTION MODEL

No	Description	Main Applied Standards
1	Initiate SSO login.	WS-Security
2	Request SAML token for internal Single Sign-On.	WS-Security & WS-Trust

3	Response by issuing SAML assertion.	WS-Trust & SAML
4	Invoke protected web service1 by using the SAML assertion.	SAML token & WS-Security
5	Authentication of the request and sends back the response.	SAML token & WS-Security
6	Acquire policy of the protected web service2 in federated zone.	WS-Metadata Exchange
7	Return policy of the protected web service2 in federated zone.	WS-Metadata Exchange
8	Ask XML firewall 1 for issuing a federated SAML token.	WS-Trust
9	XML firewall1 asks for new (federated) SAML token.	WS-Trust & WS-Federation
10	SAML authority1 asks for getting federated identity.	WS-Resource Transfer
11	Return federated identity (Pseudonym).	WS-Resource Transfer
12	Issuing new SAML token for federated identity.	WS-Trust & SAML
13	Send of request to the federated zone with new SAML token.	SAML token profile & WS-Security & WS-Federation
14	Authorization of request and sending to the federated service.	SAML token & WS-Security & WS-Federation
15	Ask for validation of SAML token and federated identity.	SAML token & WS-Security & WS-Trust & WS-Federation
16	Token validation by respect to trust relation and account linking.	SAML token & WS-Security & WS-Trust & WS-Federation
17	Send final response to the XML Firewall2.	WS-Security
18	Send final response to the XML Firewall1.	WS-Security
19	Send final response to the enterprise user.	WS-Security

The main applied web services standards have mentioned in the table above. The schema of some of the exchanged SOAP messages will be illustrated in the following. WS-Security is achieved by entering user credential in the header of the SOAP message. The schema of the SOAP message for the first step is depicted in the following figure.

```
<Envelope>
  <Header>
      .....
        <Security>
          <UsernameToken>
          <Username>EnterpriseUserName</ Username >
          <Password Type= "PasswordDigest>XY12Zabc3</ Password >
          <Nonce>123521 </ Nonce >
          <Created>2012-6-6T14:40:00 </ Created >
          </UsernameToken>
        </Security>
      .....
  </Header>
      .....
</Envelope>
```

Figure 4: SSO Login by Enterprise User

WS-Trust standard is applied for issuing, exchanging and validating security tokens by inserting required elements in the header of SOAP message. Figures 5 and 6 show the schema of the SOAP messages for exchanging and issuing of token respectively which are correspond to the steps 3 and 12 of the interaction model.

Finally the schema of the SOAP message with applying SAML token profile is shown in the figure 7 which is correspond to step 13 of the interaction model and this is the message that is sent from XML firewall1 to the XML firewall2 in the federated domain.

```
<Envelope>
    <Header>
      .....
    </Header>
      <Body>
        <RequestSecurityToken>
          <TokenType>SAML </ TokenType >
          <RequestType>ExchangeToken </ RequestType >
          <OnBehalfOf>
            <SecurityTokenReference>
Identity info of the user by referencing to the received Username Token
            </ SecurityTokenReference >
          </OnBehalfOf>
        </RequestSecurityToken>
      </Body>
</Envelope>
```

Figure 5: Request SAML Token for Protected Web Service 1 in Enterprise

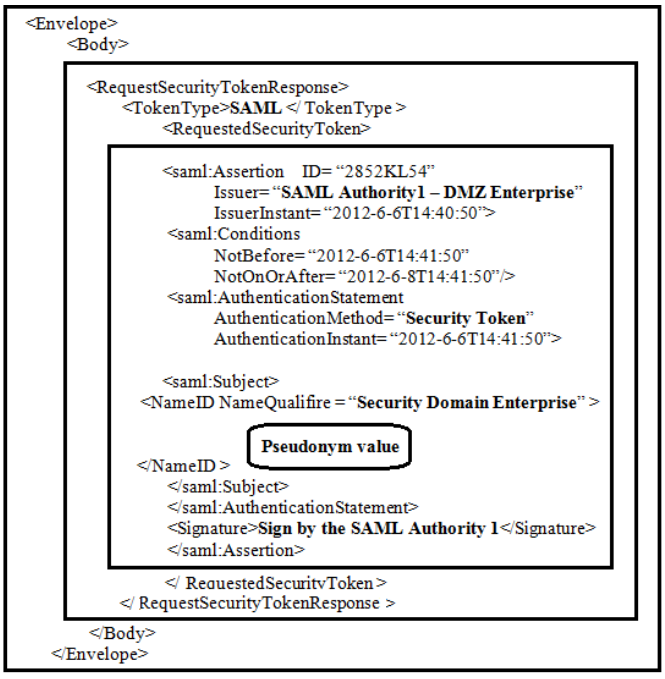

Figure 6: Issuing of Federated SAML Assertion

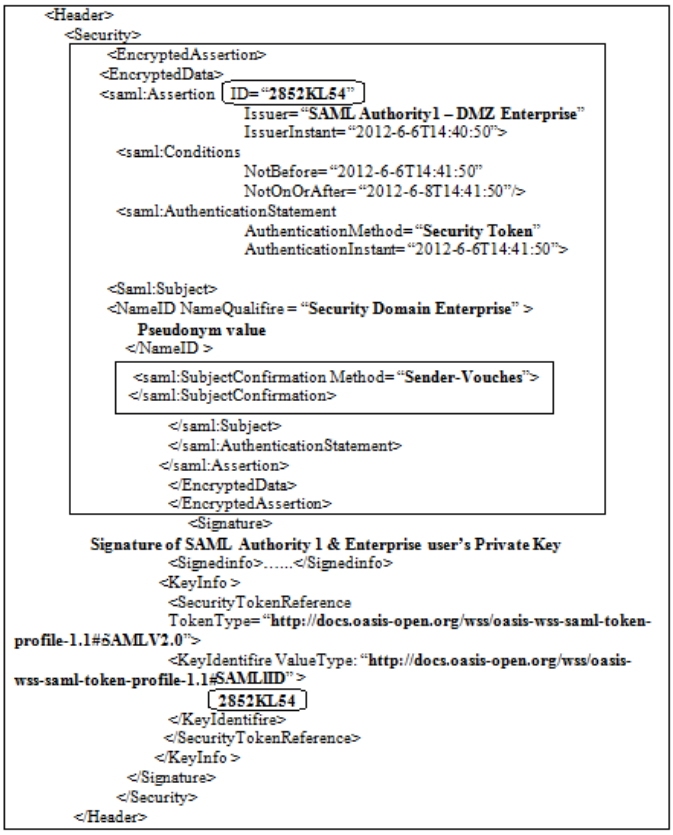

Figure 7: Encrypted Message from XML Firewall 1 to XML Firewall 2

As it can be seen, the proposed model takes advantage of SAML tokens in order to achieve web services SSO. SAML token has more benefits in comparison with applying of proprietary security tokens [16] for web services SSO. SAML token offers more flexibility and platform neutrality than proprietary token because it is based on XML that is a universal standard which has no dependency on a certain type of product. One of the key specifications in using of SAML token is representing of identity information as an assertion in XML format, it provides a baseline for interoperability of security information in loose coupling manner. Moreover, using of SAML token for authentication in web services SSO makes it easier to use XML standards such as XML Access Control Markup Language (XACML) for authorization process in web services SSO and authorization decisions can be expressed in SAML assertion based on the rules of XACML language. XACML describes XML terminology that determines the rules for making access control decisions. The XACML attribute profile explains how XACML authorization statements are supplied as the attribute statements of SAML assertions with SAML syntax, so they could be automatically mapped to XACML attributes. [15]

IV. CONCLUSION

This paper described the approach for providing web services Single Sign-On in the hierarchy model of control and automation by using SAML standard. Single Sign-On mechanism not only enhances security by improving end user password behaviors and strong authentication mechanism but also increases productivity of the system by automating access to all various applications and resources in different sections of the hierarchy model of control and automation. At the time of writing of this paper, although some standards have established for Single Sign-On approach in web environment but federated Single Sign-On for web services is not mature enough field and many researches work in order to empower this mechanism. Research challenges for federated web services Single Sign-On can be grouped in two main categories: identity federation and authentication. Identity federation challenges focus to establish the global identity that can be used across any business or enterprise. Authentication challenges have concentrated to increase functionalities of security token that is used for authentication.

In the proposed model in the section 3, federated Single Sign-On mechanism for web services was presented and pseudonym service that provides mapping mechanism for trusted identity was applied for creating federated identity between federated domains i.e. DMZ enterprise and DMZ automation which have their own identity management system and protocols for their local users and services. For authentication, the SAML token profile standard that integrates applying of SAML for web services security was used for controlling access authentication to the protected web

services by sending valid SAML assertion inside of SOAP message that indicates the identity of the service requester.

REFERENCES

[1] "Converged Plant wide Ethernet design and implementation guide", CISCO, 2010

[2] Vinay M. Igure, Sean A. Laughter and Ronald D. Williams, "Security issues in SCADA networks", Science Direct, 2006.

[3] Richard Zurawski, "Industrial Communication Technology Handbook", CRC Press, 2005

[4] François Jammes, Antoine Mensch and Harm Smit, "Service-oriented device communication using DPWS", Schneider Electric, 2006

[5] "Web Services Trust Language - WS-Trust 1.4 specification", OASIS, 2009

[6] "Web Services Federation Language - WS-Federation 1.2 specification", OASIS, 2009

[7] "Security Assertion Markup Language (SAML) version 2 Technical Overview", OASIS, 2008

[8] Skip Slone, "Identity management" white paper, The open group identity management work area, 2004

[9] Martine Linares, "Identity and Access Management Solution", SANS Institute, 2005

[10] Don Patterson, "XML firewall architecture and best practices for configuration and auditing", SANS institute, 2007

[11] François Jammes and Harm Smit, "Service-Oriented Paradigms in Industrial Automation", IEEE transactions on industrial informatics, 2005

[12] Jose L. Martinez Lastra, Ivan M. Delamer, "Semantic Web Services in Factory Automation:Fundamental Insights and Research Roadmap", IEEE, 2006

[13] Goncalo Candido, Francois Jammes, Jos´e Barata de Oliveira and Armando W. Colombo. "SOA at device level on industrial domain: Assessment of OPC UA and DPWS specification", 8th IEEE international conference industrial informatics (INDIN) , 2010

[14] Swaminathan P, Padmanabhan K, Ananthi S and Pradeep R, "The secure fieldbus (SecFB) protocol – Network communication security for secure industrial process control", IEEE region 10 conference, 2006

[15] Mark O'Neill, Phillip Hallam-Baker, "Web Services Security", McGraw-Hill, ISBN: 0-07-222471-1.

[16] Markus Hillenbrand, Joachim GÖtze, Jochen Mller, Paul Muller, "A Single Sign-On Framework for Web-Services-based Distributed Applications", IEEE 8th International Conference on Telecommunications, 2005

[17] Ronald L. Krutz, "Securing SCADA Systems", WILEY Publishing Inc, 2005

[18] Wolfgang Mahnke, Stefan-Helmut Leitner and Matthias Damm, "OPC Unified Architecture", Springer, 2009