A novel Role- and Certificate-based Single Sign-On System for Emergency Rescue Operations

Thang Tran, Mohamad Sbeiti and Christian Wietfeld
Communication Networks Institute (CNI)
Faculty of Electrical Engineering and Information Technology
TU Dortmund University, Germany
Email: {Thang.Tran, Mohamad.Sbeiti, Christian.Wietfeld}@tu-dortmund.de

***Abstract*—In large scale disaster management operations with hundreds and thousands of victims, fast access to distributed heterogeneous information of different organizations is required for efficient and reliable dispensation of rescue operations. The development of such emergency systems poses a big challenge, if requirements such as performance, security and reliability have to be simultaneously fulfilled. In this paper, we propose a novel Role integrated Certificate-based Single Sign-On (RC-SSO) solution for fast mobile access between first responders at the incident scene and their distributed organizations. Besides the illustration of operational details of the RC-SSO solution, we validate our concept by implementing an experimental prototype as proof-of-concept for a limited number of users. Furthermore, we design a simulation model to determine the performance boundary of our solution under high user density. In contrast to other related emergency system solutions, our approach does not employ a so-called Identity Provider (IDP) for authentication and authorization process and thus reduces additional communication cost as well. A comparison of our proposed solution to an IDP based classical single sign-on counterparts i.e. Security Assertion Markup Language (SAML) shows that our RC-SSO outperforms these by up to 80%. In addition, RC-SSO ensures high data security level with negligible overhead compared to the standard security protocol SSL/TLS.**

I. Introduction

A. Motivation

Large scale disasters like the earth quakes in Haiti or floods in Pakistan involved several thousands of victims. Such extraordinary events demand an efficient disaster response management, especially if thousands of first responders of heterogeneous organizations (e.g. fire departments, police, Red Cross societies, agencies for technical relief, etc.) are in action at the incident scene. In such a scenario, a huge amount of information has to be managed and exchanged by various organizations. However, since each organization uses its own organization-specific system and these are incompatible to each other, essential and latest information is not available in time at the incident scene [1]. The latter is crucial and has a huge influence on the success of the operations. Therefore, we proposed in [2] a new federation system concept which utilizes a XML based Protection and Rescue Markup Language (PRML) as a common data model for information exchange between public institutions as well as private companies. This has the advantage that legacy systems can coexist using PRML.

B. State-of-the-art Analysis

Related federation system solutions are usually based on a Federated Identity Model (FIM) [3], used for authentication and authorization, and illustrate an approach that enables the secure interoperability between heterogeneous information systems. Additionally, FIMs offer a function called Single Sign-On (SSO) where user requires to be authenticated only once to get access to all authorized services. There currently exist three famous models for implementing federated identity: Security Assertion Markup Language (SAML) [4], OpenID [5] and Microsoft Cardspace [6]. SAML is the most mature and comprehensive technology and has undergone standardizations in 2002 (SAML 1.1) as well as in 2005 (SAML 2.0), respectively [7].

In [8], we proposed a SAML based mobile Emergency Response System (mERS). The *mERS* solution uses an Identity Provider (IDP) representing a server that authenticates users and manages their access rights. Due to the property of FIM and the dependence on IDP, additional communication procedures are needed and will result in lower system performance. Thus, we proposed a solution by using a different SAML Binding to obtain better performance in [9], nonetheless an IDP is still required because of the SAML specification. Alternative solutions as introduced in [10] and [11] present approaches without an IDP applying X.509 certificates for authentication only. These approaches need an intermediate server component to manage the authentication and authorization processes between clients and Service Providers (SP). In [12], a related authentication method with a role based access control using X.509 certificate is suggested where the authentication and authorization procedures between clients and offered applications are controlled by a so-called Multi Agent System (MAS). This approach employs an additional attribute certificate for authorization besides a client certificate.

In order to reduce the dependencies (e.g. IDP) and to fulfill the operational requirements (i.e. performance and security) of a modern emergency response system, we propose a cost-efficient and deployable solution for Emergency Personnels (EPs) (e.g. firefighter). This approach allows efficiently and securely search and retrieve information from a federated IT-system of different organizations while they are on move. As a mobility solution for EPs, we recommended in [13]

Link to published version: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5962864

a Client based Secure Vertical Handoff solution for Mobile Units (CSH-MU). The main advantage of our novel mobile Disaster Response System (mDRS) is that each organization keeps on using its own software to access and work with the organization-specific data. Furthermore, in contrast to the above mentioned related solutions, a client of EP can directly access to the information system of public authorities and other rescue organizations (i.e. information retrieval). In terms of security, authentication and authorization are handled by our Role integrated Certificate-based Single Sign-On (RC-SSO) solution. This approach represents an alternative to classical standard SSO solutions for time critical applications (e.g. disaster management operations, fire missions). Integrated in the certificate, a predefined role enables communication partners to identify each other in a trusted federation. Moreover, the roles describe access rights and define the filtering rules for information retrieval at the corresponding organization. Our approach has the property that the authorization information is already integrated in the mutual authentication process using SSL/TLS protocol [14].

Due to this fact, the overhead of RC-SSO is negligible compared to the standard security protocol SSL/TLS. We have thereby a technical low cost solution while meeting all security requirements of first responders within the mDRS-federation.

The rest of the paper is structured as follows: Section 2 briefly presents the system architecture of mDRS and the communication procedure of RC-SSO. As a proof of concept, we implement a mDRS prototype and discuss the results of the performance evaluation in section 3. In the latter, we also shortly describe a simulation model for mDRS with RC-SSO and Security Assertion Markup Language (SAML), respectively. Based on the simulation results, we compare the performance behavior of our solution with a classical SSO solution depending on high number of users, followed by a conclusion in section 4.

II. Mobile Disaster Response System (mDRS)

This section describes the basic concept of mDRS where the focus lies more on RC-SSO. For detailed information about the different components of mDRS and its services, we refer to [2].

A. System Architecture

The model of mDRS consists of two major components for the interconnection between different organizations: Entities and Agents (see Fig. 1). An Agent describes a set of mandatory and optional services. Mandatory services include all basic services which are required to fulfill a specific role of an organization. For instance, mandatory services have to establish the connection within the federation, control the authentication and authorization process (RC-SSO), and have to handle the requests for information from other organizations. The Entity is basically a set of Agents and represents stationary or mobile organizations (e.g. Fire Department, Hospital) providing emergency information to trusted partners in the mDRS federation. As a common data model, we developed the Protection and Rescue Markup Language (PRML) guaranteeing the interoperability of secure information exchange between different trusted Entities [2].

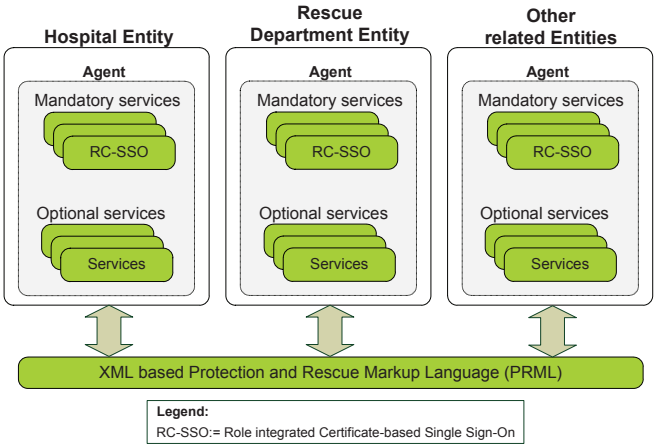

Fig. 1. System Architecture of mobile Disaster Response System (mDRS)

B. Role integrated Certificate-based Single Sign-On (RC-SSO)

This section briefly introduces the communication procedure of RC-SSO in terms of the interaction between different entities. The process is described with reference to Figure 2. It should be noted that the RC-SSO solution can be used by an emergency client or entity to directly access the offered service of different entities.

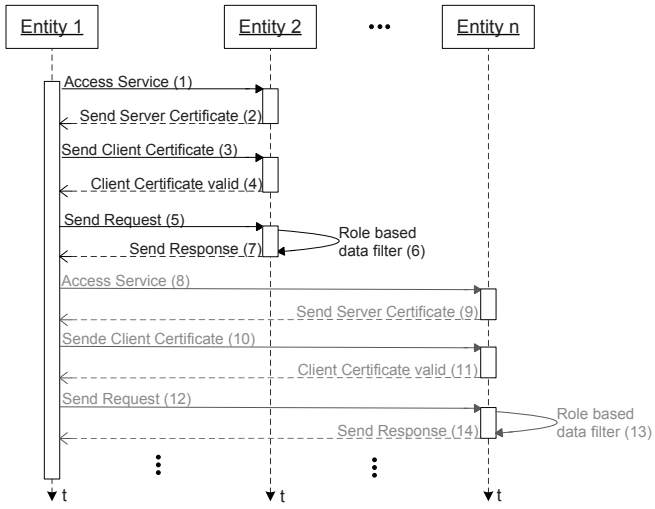

Fig. 2. Communication Procedure of RC-SSO

When an entity or client wants to request emergency information, a SSL/TLS communication procedure is started between the entities at first. In order to check out the authenticity of the communication endpoints, the server and the client send their X.509 based identity certificates to the communication partner. To minimize the number of communication procedures, we directly integrate the predefined role of an organization as additional information to the extensions of client's

X.509 (messages 1, 2, 3 & 4 in Fig. 2). This information is later on used for the authorization. After the successful mutual authentication, the client transmits the information request to the server (e.g. Entity 2, see Fig. 2). Since the client has already sent its certificate, the server reads out the role and decides depending of its policy which data can be transferred back to the client (e.g. Entity 1, see Fig. 2) (messages 5, 6 & 7 in Fig. 2). In our solution the server does not need to create an additional SSL/TLS connection to an Identity Provider for requesting the access rights of the client compared to a classical federated identity model.

The certificates are issued by a trustable Certificate Authority (CA). In Germany, the *Federal Office for Information Security* is a possible CA for emergency and crisis relief forces. The administration effort of the RC-SSO certificates is low in comparison to other CAs like VeriSign that operates a lot of different arrays of network infrastructure. In case of a crisis relief forces, it is a fact which organizations are involved and information is essential required for an efficient rescue operation. Moreover, only predetermined EPs (e.g. crisis management group, on-scene commander, emergency doctor) are allowed to use the mDRS. In order to guarantee the seamless communication between the entities, a set of minimum roles are predefined in the trusted mDRS federation. Roles describe the operational hierarchy of emergency organizations. A certificate usually includes only one role, which completely satisfies emergency requirements. Notably, authorized EPs are able to sign on from multiple sites using mDRS in order to guarantee the flexibility during the rescue operations.

We assume in this paper that role integrated certificates are well protected and are not prone to theft or physical attacks. Certificate revocation mechanisms will be considered in a future work.

III. Performance Evaluation

A. Experimental Results

To inspect the performance degradation limit imposed by our approach in comparison to a non-secure communication and a standard SSL/TLS communication between one mobile client and a server respectively, we have implemented a real test bed.

TABLE I
Technical description of the test bed components

Client	
Hardware	Lenovo Thinkpad T500 Intel Core2 Duo CPU T9550, 2.66GHz 2 GB RAM
Software	Microsoft Windows XP Professional, Service Pack 3 Apache JMeter 2.4 Netbeans 6.8 with Java 1.6.0_18
Server	
Hardware	Intel Core2 Duo CPU E6750, 2.66GHz 4 GB RAM
Software	Ubuntu 9.10 Karmic Koala Netbeans 6.8 with Java 1.6.0_20

The results obtained by this test bed have been then fed into a simulation model to track the variation of this limit by a higher number of users. The test bed consists of two components: one server and one client. Each of them composed of a hardware as well as a software part. A detailed description of both components is illustrated in Table I.

Both client and server are located in different networks. Using a web browser the client requests a web service deployed on the server 100 times via WiFi (54Mbit/s). We apply WiFi since this technology is used in emergency situations as an alternative to establish a highly reliable network at the incident scene. In such a situation, public communication infrastructures usually break down. For detailed information, we refer to [15].

The server in our test bed corresponds to a hospital entity developed within the German project SPIDER [1]. Among other services, this entity implements the *getAvailableResources* web service. We used this service as a reference service in our test bed. By calling it, the hospital entity reads information out of its database about current available medical resources at the hospital and sends them back to the client.

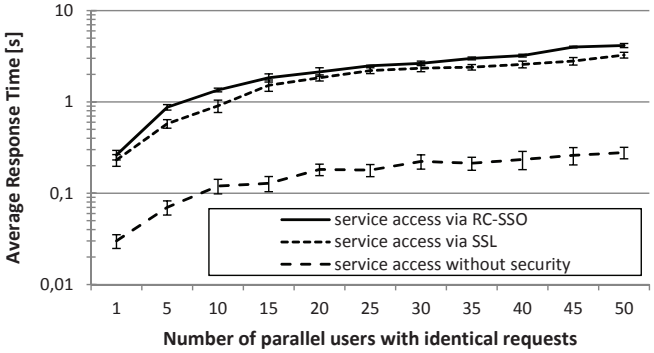

Fig. 3. Comparison of average response time with confidence interval measured under experimental conditions

Figure 3 illustrates the average response time with an increasing number of simultaneous clients. In order to illustrate the accuracy of the average response time, the confidence intervals are plotted for which the corresponding average value is 99% in the measured interval. To determine the performance values, a traffic emulator JMeter [16], running on the client, is used to emulate the number of users with parallel and identical requests to the web service.

We distinguish in Figure 3 between three scenarios for service access depending on the communication security level:

- In scenario *A* no communication security has been applied and the packets are transmitted bare over HTTP.
- In scenario *B*, the client establishes a SSL/TLS connection before requesting the emergency service.
- Scenario *C* corresponds to our mDRS with RC-SSO solution. In addition to the SSL/TLS connection, the server first reads the client role out of the certificate before processing its request. The role is used for the authorization process and describes the access rights of a

user.

These three scenarios are necessary to acquire a thorough analysis of the impact of our approach on the communication performance. As expected the time required in scenario *C* is higher than the time needed in *A* and *B* due to the higher security level of RC-SSO (see Fig. 3).

In order to guarantee the start of parallel request at same time as a worst case scenario, only 50 clients are emulated with JMeter. Therefore, further investigations with higher number of clients are provided in the next section.

B. Simulative Analysis

In order to analyze the system performance and behavior of RC-SSO relating to the specific number of users and used security mechanisms, a simulation model is implemented using the discrete event-based simulation environment of OMNeT++4.0 [17]. Figure 4a illustrates the simulation model of

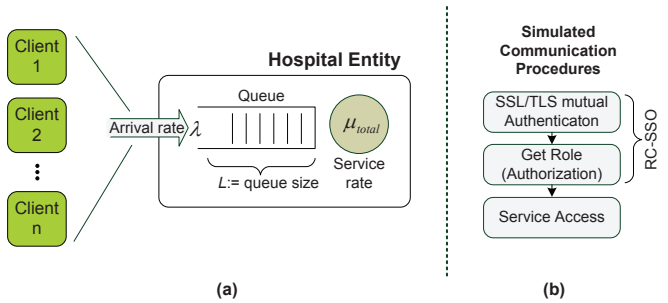

Fig. 4. (a): Simulation model of RC-SSO with service access to hospital capacity. (b): Simulated communication procedures

RC-SSO with incoming requests of users representing by the arrival rate λ. The receiving requests are put into the queue with queue size *L*=100 demonstrating the number of threads that an Entity (see Fig. 4: hospital entity) can handle. The processing order of the requests in the queue is executed by the First-In-First-Out (FIFO) principle. In our simulation, we considered the worst case scenario where a specific number of users start the identical requests at same time. In this case the interarrival time is zero. Moreover, the users resend the requests until the retrieval is executed successfully. Based on measured mean values from the experimental results and the assumption that the service rate has an exponential behavior [18] depending of rising number of users, the processing time of a communication procedure is described by the total service rate μ_{total} defined by the following equation:

$$\mu_{total} = \mu_{auth} + \mu_{role} + \mu_{serv} \quad (1)$$

$$\mu_{auth} = (0.187 - 1) + e^{n \cdot c} \quad (2)$$

$$\mu_{role} = (0.018 - 1) + e^{n \cdot c} \quad (3)$$

$$\mu_{serv} = (0.016 - 1) + e^{n \cdot c} \quad (4)$$

The parameter *n* in equation 2, 3 and 4 represents the number of users and *c* is a fix correction value as start value, which is set to 0.0001 in our simulation scenario, for a scenario with one user client. The values 0.187s, 0.018s and 0.016s are the measured service rates for one user. In our simulation model, the communication procedure starts with the SSL/TLS mutual authentication (μ_{auth}). After this step, the authorization process reads out the role name from the identity certificate (μ_{role}). When the authentication and authorization procedure are successfully accomplished, the service for requesting the capacity of the hospital can be accessed (μ_{serv}) (see Fig. 4b).

In order to validate our proposed simulation model, we compared the experimental and simulation results. Figure 5 depicts the average response time measured by the test bed and obtained by the simulation model. It is shown that the simulation results closely resemble the corresponding curves of the experimental measurements (scenario B and C).

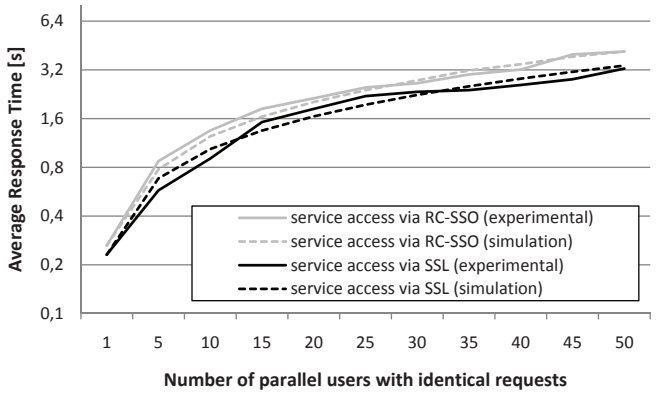

Fig. 5. Comparison of average response time measured under experimental conditions and simulation

Figure 6 shows the simulation results based on a worst case scenario where a specific number of users send parallel and identical requests. The results demonstrate that the average response time increases up to 18% more with RC-SSO compared to scenario B with SSL/TLS. It should be noted that scenario B only includes the authentication process, whereas RC-SSO consists of the mutual authentication and authorization. Moreover, the analysis results exposed that the influence of security mechanism increases the average response more than 90%, whereby the SSL/TLS communication has a high influence on the average response time.

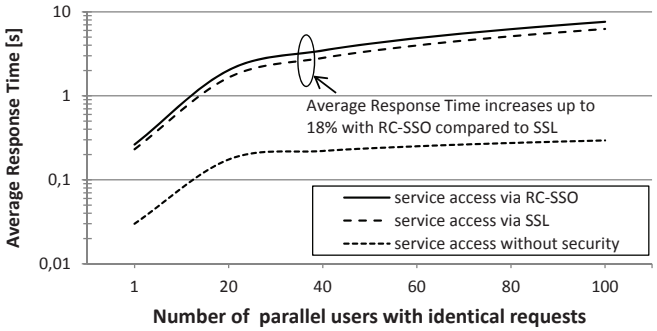

Fig. 6. Comparison of average response time measured under three different simulation scenarios, namely with RC-SSO, SSL/TLS and without security

FIM-based solutions such as SAML are typically applied to enable the seamless interoperability between distributed service providers with SSO feature. However, these solutions are not applicable for time-critical applications. In order to compare our RC-SSO approach to an emergency response system with SAML Redirect/Post-Binding, which is the mostly used profile, we also have developed a discrete event-based simulation model in the OMNeT++ environment simulating the communication process of SAML Redirect/Post-Binding [4] based on the model shown in Figure 7. The simulated procedure starts with the service request at the Hospital Entity (HE). Since the user is not authenticated, the client is then redirected to the IDP. After the successful authentication, the IDP creates a SAML assertion that asserts the authenticity of the user. In the next step, the IDP forwards the user together with the assertion to HE. In order to proof the assertion and to receive the access rights (attributes) of the user, HE contacts IDP directly. When the authorization and proof of identity are successful, the user/client can finally access the service. The communication steps are numbered illustrated in Figure 7.

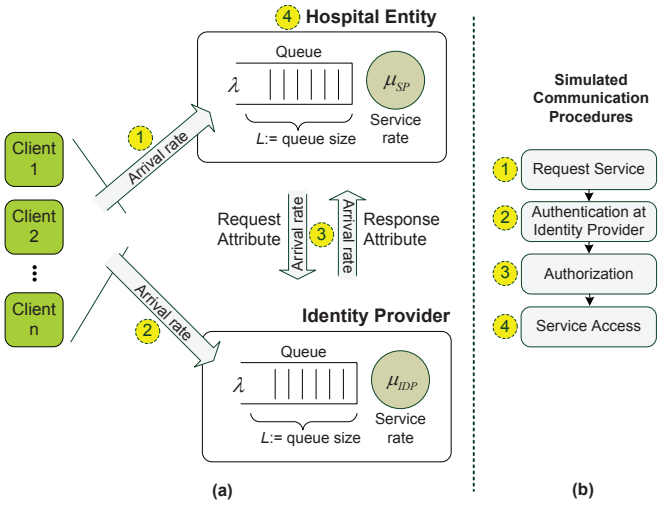

Fig. 7. (a): Simulation Model of SAML Redirect/Post-Binding with service access to hospital capacity. (b): Simulated communication procedures

The configuration parameters of the SAML model are set as follows:

$$\mu_{idp} = (0.205s - 1) + e^{n \cdot c} \quad (5)$$

$$\mu_{sp} = \mu_{samlRole} + \mu_{serv} \quad (6)$$

$$\mu_{samlRole} = (0.388s - 1) + e^{n \cdot c} \quad (7)$$

$$\mu_{serv} = (0.016s - 1) + e^{n \cdot c} \quad (8)$$

The equation 5 represents the service rate for authentication. μ_{sp} consists of the required time for authorization ($\mu_{samlRole}$) and service access (μ_{serv}). The correction value c is set to 0.0001. In order to obtain the service rate for the SAML model, we extended our test bed by a second server with the same components described in Table I for the first server. In this case, the second server represents an Identity Provider managing the authentication and authorization procedures. Moreover, we used JMeter to emulate 50 users with identical requests at the same time. Furthermore, we assume that the queue size is 100 and the requests of a specific number of users start concurrently in our SAML model. The lost requests, which are sent by the clients, are transmitted till such time as successful reception and execution. To validate the parameterization, we compared the experimental and simulation results that closely approximate to the curve of the experimental measurement (see Fig. 8).

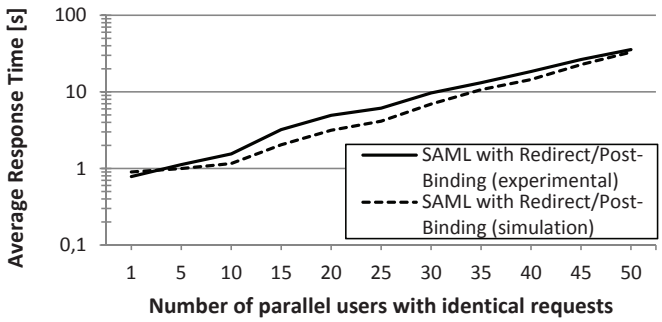

Fig. 8. Comparison of average response time of SAML Redirect/Post-Binding measured under experimental conditions and simulation

According to Figure 9, the average response time using SAML increases up to 80% compared to RC-SSO. The reason for this behavior is because of the additional communication procedure of SAML. The creation of a secure communication channel applying SSL/TLS usually requires most of the time. In case of SAML, the client has to create a SSL/TLS channel to HE and then to the IDP for authentication. Moreover, HE also establishes a SSL/TLS connection to IDP for attribute retrieval. Especially interesting to note from Figure 9 is the fact that the response time of SAML ranges for a higher number of 35 users in an unexpectable interval (>10s).

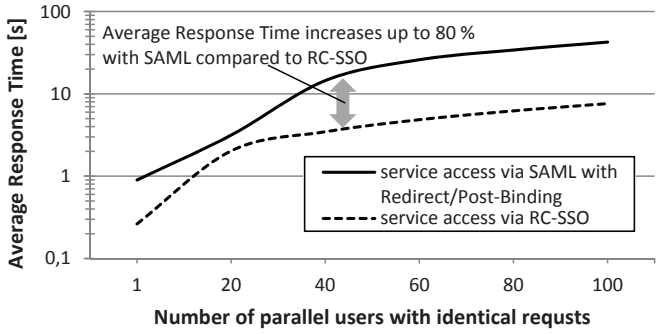

Fig. 9. Comparison of average response time of SAML Redirect/Post-Binding and RC-SSO using simulation models

To sum up, the simulation results show that RC-SSO performs better than a classical FIM solution such as SAML and is therefore more suitable for time-critical emergency rescue operations. In contrast to SAML, RC-SSO is based on the SSL/TLS specification for mutual authentication where information for authorization is already integrated in the client

certificate so that the authorization process can be directly executed on server side without exchanging any additional messages with the client. This means no changes in the SSL/TLS standard and no third server component like the IDP are necessary. Due to this fact, our approach ensures the interoperability and represents a cost-efficient solution.

IV. Conclusion and Future Work

In this paper, we proposed a mobile Disaster Response System (mDRS) with an effective Role integrated Certificate-based Single Sign-On (RC-SSO) solution. This solution enables responders at the incident scene fast and secure access to distributed service providers. As a proof of concept, two mDRS prototypes built on RC-SSO and SAML have been implemented for the secure communication within that trusted federation. SAML represents a classical Federated Identity Model (FIM) for enabling the seamless interoperability of the distributed trusted service providers.

In order to analyze the system performance of both solutions under high user density, two discrete event-based simulation models have been developed where the simulation results are validated by the measured values obtained from a real test bed. The experimental and simulation results illustrated that RC-SSO performs up to 80% better compared to the SAML approach and is therefore more suitable for emergency applications. In contrast to a classical FIM, our approach does not need an intermediate server component such as the IDP in a trusted federation. Thus, additional communication procedures and the technical cost can be reduced.

In future work, we plan to investigate our mDRS system in an experimental field test employing a small number of users. Furthermore, we intend to thoroughly evaluate its security using practice oriented provable security methods. Apart from that, we designate to compare our RC-SSO solution with its counterparts in the single sign-on field. Moreover, we aim to evaluate the applicability of conventional revocation list mechanisms for our solution and to optimize them in order to meet performance goals and feasibility constraints of rescue operations.

Acknowledgment

The authors would like to thank Giuseppe Tabbi for his technical assistance. Our work has been conducted within the SPIDER project (Security System for Public Institutions in Disastrous Emergency scenaRios), which is part of the nation-wide security research program funded by the German Federal Ministry of Education and Research (BMBF) (13N10238).

References

[1] German Research Project, http://www.spider-federation.org, 2010.

[2] Subik, S., Rohde, S., Wietfeld, C., Weber, T.: *SPIDER: Enabling Interoperable Information Sharing between Public Institutions for Efficient Disaster Recovery and Response*, IEEE International Conference on Technologies for Homeland Security, pp. 190-197, Waltham, MA, USA, November 2010.

[3] Bhatti, R., Bertino, E., Ghafoor, A.: *An integrated approach to federated identity and privilege management in open systems*, Communications of the ACM, pp. 81-87, vol. 5, New York, NY, USA, February 2007.

[4] Ragouzis, N., Hughes, J., Philpott, R., Maler, E., Madsen, P., Scavo, T.: *Security assertion markup language (saml) v2.0 technical overview*, Security Services Technical Committee of OASIS, 2008. http://www.oasisopen.org.

[5] Recordon, D., Reed, D.: *Openid 2.0: a platform for user-centric identity management*, In DIM 06: Proceedings of the second ACM workshop on Digital identity management, pp. 11-16, New York, NY, USA, October 2006.

[6] Bhargavan, K., Fournet, C., Gordon, A. D., Swamy, N.: *Verified implementations of the information card federated identity-management protocol*, Proceedings of the ACM symposium on Information, computer and communications security, pp. 123-135, New York, NY, USA, March 2008.

[7] Maler, E., Reed, D.: *The venn of identity: Options and issues in federated identity management*, IEEE Security and Privacy, vol.6, no.2, pp. 16-23, March-April 2008.

[8] Tran, T., Yousaf, F. Z., Wietfeld, C.: *RFID Based Secure Mobile Communication Framework for Emergency Response Management*, IEEE Wireless Communications and Networking Conference (WCNC), IEEE, pp. 1-6, Sydney, Australia, April 2010.

[9] Tran, T., Wietfeld, C., *Approaches for Optimizing the Performance of a Mobile SAML-based Emergency Response System*, IEEE Enterprise Distributed Object Computing Conference Workshops (EDOC), pp. 148-156, Auckland, New Zealand, September 2009.

[10] Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: *A Robust Single Sign-On Model Based on Multi-Agent System and PKI*, Sixth International Conference on Networking (ICN '07), pp. 101-106, Sainte-Luce, Martinique, April 2007.

[11] Nobayashi, D., Nakamura, Y., Ikenaga, T., Hori, Y.: *Development of Single Sign-On System with Hardware Token and Key Management Server*, Second International Conference on Systems and Networks Communications (ICSNC), pp.73-73, Cap Esterel, French Riviera, France, August 2007.

[12] Fugkeaw, S., Manpanpanich, P., Juntapremjitt, S.: *AmTRUE: Authentication Management and Trusted Role-based Authorization in Multi-Application and Multi-User Environment*, The International Conference on Emerging Security Information Systems and Technologies, (SecureWare), pp. 216-221, October 2007.

[13] Tran, T., Yousaf, F. Z., Wietfeld, C.: *CSH-MU: Client Based Secure Handoff Solution for Mobile Units*, 21st IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC), IEEE, pp. 2259-2263, Istanbul, Turkey, September 2010.

[14] Dierks, T., Rescorla, E.: *The Transport Layer Security (TLS) Protocol Version 1.2*, Request for Comments 5246, Internet Engineering Task Force, August 2008.

[15] Wolff, A., Subik, S., Wietfeld, C.: *Performance analysis of highly available ad hoc Surveillance Networks Based on Dropped Units*, IEEE Technologies for Homeland Security Conference, pp. 123-128, Boston, MA, USA, May 2008.

[16] J. A. Project: *Apache JMeter*, Apache Project Homepage: http://jakarta.apache.org/jmeter

[17] Varga, A.: *The OMNeT++ Discrete Event Simulation System*, Proceedings of the European Simulation Multiconference, pp. 319-324, Prague, Czech Republic, June 2001.

[18] Abdelzaher, T.F., Shin, K.G., Bhatti, N.: *Performance guarantees for Web server end-systems: a control-theoretical approach*, IEEE Transactions on Parallel and Distributed Systems, pp. 80-96, vol. 13, January 2002.