

Task Proposal (SP-1)

expecting P4 level

1. Task Proposal

- 1.1. Task Proposal ID: 15/DS -001
- 1.2. Task Title: Expert – Authentication and Authorization Specialist
- 1.3. Requestor / Division / Section: Andreica Dorin_Paul / SGIS / DS
- 1.4. Task Proposal Type: CFE Task
- 1.5. Task Category: D (Information Processing)
- 1.6. Reason (if task is either a joint task or desires multiple acceptance)

2. Project

- 2.1. Project ID and Title: SGIS-003 - Safeguards Information Systems and System Usability
- 2.2. Project Manager / Division / Section: Whitaker Gregg / SGIS / PS

3. Safeguards Requirement Identification

3.1. Background

The function of verifying a user's identity — known as authentication — is important in establishing trust in critical business processes. In its simplest form, authentication is the act of verifying a person's claim on his or her identity and is usually implemented through a username and password combination when logging into an IT system or application. There are multiple ways by which users can provide their identity, such as typing a username and password, swiping a smart card, waving a token device, or using voice recognition. In fact, the basis of authentication lies in the principle that without a proper form of identification, a system will not be able to correlate an authentication factor with a specific subject. The proper identification of a person, device, or group is vital for safeguarding and maintaining the confidentiality, integrity, and availability of the IT infrastructure and sensitive data.

3.2. What is Needed and When

The Identity and Access Management Specialist is needed immediately.

3.3. Why is the task needed and consequences if task is not performed

The task is needed to evaluate and improve of role based authentication and authorization technical solution adopted in the department of safeguards. If not performed confidentiality, integrity, and availability of the IT infrastructure and departmental data repositories will be jeopardized.

3.4. How will the task results be used and by whom

The task results will be used by all Information and Communication Technology solution providers in the Department of Safeguards to implement appropriate authentication and authorization mechanism for proper identification of a person, device, or group. It is vital for safeguarding and maintaining the confidentiality, integrity, and availability of the IT infrastructure and departmental data repositories.

4. Proposed Sub Tasks

5. Proposed Work Outline

- 5.1. Estimated Duration (months): 24
- 5.2. Status Report Frequency: Once every 3 Month
- 5.3. Supporting Divisions(s) / Section(s): SGIS / DS , SGIS / IS , SGIS / PS , SGIS / USS
- 5.4. End User Divisions(s) / Section(s): SGCP / CPC
- 5.5. Proposed Work Phases

Phase Number: 1

Phase Title: Produce Work Plan

Description

Work Plan will be created consulting with the Expert by taking his/her experience and knowledge into account.

Start Month after acceptance: 1 End Month: 1

Carried out in sub tasks:

Phase Number: 2

Phase Title: Implementation

Description

- Evaluation and improvement of role based authentication and authorization technical solution
- Configuration and hosting of web applications and services with IIS
- Work with
 - technical leads to integrate the solution into their applications
 - authorization support team to explain how to modify authorization rules

- data owners to explain how to generate authorization reports
- risk and security team to develop technical authorization policies

Start Month after acceptance: 2 **End Month:** 24

Carried out in sub tasks:

6. Safeguards Approval Process

6.1. Suggested to MSSPs: FRA, GER, UK, USA

6.2. Reason for suggestion of MSSPs

The suggested MSSP have expertise in software engineer and the related technical competencies to support the requests.

7. Attached Documents

N/A

Job Description Cost-Free Expert

Functional Title:	Expert - Authentication and Authorization Specialist (15/DS-001)
Grade:	P4
Organizational Unit:	Application Development Team Development Section Office of Information and Communication Systems Department of Safeguards
Occupational Group:	1A05 - Computer Information Systems Specialists

Organizational Setting

The Department of Safeguards (SG) is the organizational hub for the implementation of IAEA safeguards. The IAEA implements nuclear verification activities for some 180 States in accordance with their safeguards agreements. The safeguards activities are undertaken within a dynamic and technically challenging environment including advanced nuclear fuel cycle facilities and complemented by the political diversity of the countries.

The Department of Safeguards consists of six Divisions: three Operations Divisions: A, B and C, for the implementation of verification activities around the world; three Technical Divisions: Division of Concepts and Planning, Division of Information Management, and Division of Technical and Scientific Services; as well as two Offices: the Office of Safeguards Analytical Services and the Office of Information and Communication Services.

Within the Department of Safeguards, the Office of Information and Communication Systems (SGIS) is the centre of competence for the specification, development and maintenance of Information and Communication Technology (ICT) systems and for the management of all ICT infrastructure and services to support safeguards. In partnership with other organizational entities, SGIS is responsible for planning and implementing an ICT strategy as well as enforcing ICT standards.

The Development Section provides ICT services to the Department of Safeguards and Member States, working cooperatively with staff in the Operations Divisions and the Technical Divisions to plan, establish and maintain information systems. The Section specializes in providing system analysis, software design, and implementation and maintenance services. The Section follows and implements best practices in the areas of software engineering, project management and quality management and continuously monitors the Department's information related needs so that they can be met through requests for new or enhanced ICT solutions.

Main purpose

Under the general supervision of the Head of the Development Section, and reporting to the Team Leader for the Application Development Team, the Identity and Access Management Specialist carries out the evaluation, implementation and maintenance of authorization systems for the Department of Safeguards.

Role

The Identity and Access Management Specialist is: (1) *an expert* for IT identity and access management systems; (2) *a business analyst*, working with project teams and user to establish and unify authorization standards; (3) *a project manager*, defining, planning and making a business case in the area of authorization systems; (4) *a senior software engineer*, specifying and implementing system to system interfaces and customizing authorization systems.

Partnerships

The Identity and Access Management Specialist works closely with various project teams to understand their

Job Description Cost-Free Expert Identity and Access Management Specialist

requirements and assists in finding the most appropriate solution. The Identity and Access Management Specialist collaborates with colleagues in SGIS that are responsible for the infrastructure (middleware, service monitoring, networking, etc.), software engineering (standards, guidelines, etc.), and business analysis (business process).

Functions / Key Results Expected

- Evaluate, simplify and improve our existing role based authentication and authorization technical solution
- Provide technical assessments and recommendations
- Develop detailed security documentation
- Deep knowledge of RBAC and ABAC approaches
- Experience with security technologies like NTLM, Kerberos, SAML
- Experience with .NET security implementation
- Configuration and hosting of web applications and services with IIS
- Work with technical leads to explain how to integrate the solution into their applications
- Work with the authorization support team to explain how to modify authorization rules
- Work with data owners to explain how to generate authorization reports
- Work with risk and security team to develop technical authorization policies
- Develop technical documentation on identity and access management for various stakeholders (e.g. technical leads, support team, security team)

Knowledge, Skills and Abilities

- *Technical expertise:*
 - In-depth knowledge of system analysis and design, object oriented programming and service oriented architecture principles.
 - Strong expertise in the area of IT authorization technologies and standards.
 - Detailed knowledge of network configurations and security standards.
 - Professional skills in software engineering tools, web service technologies, object oriented programming languages, web technologies, middleware, and database management systems.
 - Strong knowledge of information security and secure coding techniques.
 - Familiarity with international safeguards, nuclear material accounting, verification activities and State-supplied data handling an asset.
- *Analytical skills and customer orientation:* Ability to analyse business processes and translate customer requests into ICT solutions.
- *Interpersonal skills:* Ability to establish and maintain good relationships with internal and external counterparts and to work harmoniously in a multicultural/multidisciplinary team with respect and sensitivity for diversity.
- *Communication skills:* Ability to write clearly and in a structured manner and to make effective oral presentations.
- *Knowledge management:* Openness to new ideas, technologies and tools in the IT industry and a willingness to learn and share skills and knowledge.
- *Teamwork:* Proven ability to work effectively as a member or leader of a multinational team with respect and sensitivity for diversity.

Education, Experience and Language Skills

- University (or equivalent) degree in computer science or a related field.
- Minimum of five years of relevant practical experience in managing and customizing IT Authorization solutions.
- Having advanced certifications in security, identity and access management is an asset (e.g. CISSP)
- Experience in all aspects of software engineering processes with demonstrated abilities in following formal software methodologies and a disciplined approach to software engineering.
- Fluency in written and spoken English. Knowledge of another official IAEA language (i.e. Arabic, Chinese, French, Russian, Spanish) an asset.