**Ontology Modeling Document**

The ontology has been modeled utilizing the OWL language to represent the components of the Secured Innohub platform. A taxonomy was created that divides the platform's components into six macro-areas (classes): Front End, Back End, Knowledge Base, Services, Tools, and Development Libraries. The individual components of the platform are represented as Individuals in the Secured Knowledge Graph (KG). The relationships between two or more components are represented using *Object Properties*, while the functions specific to each component, along with technical specifications and Role-based access control (RBAC) rules that permit access, are represented via *Data Properties*.

Whenever a property is common to all components of a macro-area in the platform, the `owl:equivalentClass` is used to assign this property to all the Individuals in the corresponding class.

Outside the `Secured_Innohub` class, two Individuals are defined: `user` and `external_data_source`. These entities interact with the platform's components through specific object properties, notably those related to login processes and access to platform resources. An SWRL rule has been implemented to condition the user's access to resources on possessing an appropriately leveled RBAC token. However, since detailed access rules for individual platform resources are not yet available, the SWRL rule is currently configured to allow unlimited access to the user.

To model potential cybersecurity threats to the platform, databases in .csv format from CAPEC (Common Attack Pattern Enumerations and Classifications) and CWE (Common Weakness Enumeration), both maintained by the MITRE Corporation, were used. The CWE database also provided information on the associations between CWE vulnerabilities and those present in the CVE (Common Vulnerabilities Enumeration) database, curated by NIST. The vulnerabilities and attack patterns obtained from these databases are presented in the Secured KG as Individuals within the CAPEC, CWE, or CVE classes.

The `CAPEC`, `CWE`, and `CVE` classes, along with some of their descriptive and relational properties, were partially imported from the OdTM (Ontology-driven Threat Modelling) ontology set. The classes were imported from the OdTM Integrated Model, and the properties from the OdTM Base Threat Model.

The `CAPEC` class is subdivided into six subclasses, each categorizing attack patterns by domain of attack. To reflect this classification within the KG, the attack pattern hierarchy was reconstructed using the transitive object properties `childOf` and `parentOf`, along with `peerOf`, `canFollow`, and `canProceed` to clarify the relationships between attack patterns.

The attack patterns are associated with data properties that describe their level of abstraction, purpose, impact on information systems, probability (based on ease of execution), typical severity, and suggested strategies for mitigating the risk.

From the CWE database, information was gathered regarding the relationships between CAPEC attack patterns, CWE weaknesses, and CVE vulnerabilities. The weaknesses are also described with a set of properties similar to those associated with the CAPEC attack patterns, differing only in the absence of information about the probability of attacks and the severity of damage.

The `CWE` class contains several subclasses representing lists of vulnerabilities categorized by danger and frequency, compiled by MITRE and CISQ. The Individuals of the CAPEC and CWE classes are accompanied by textual descriptions and notes, while the Individuals of the CVE class contain only descriptions.

The attacks and vulnerabilities in the CAPEC, CWE, and CVE classes are linked to the individual components of Secured Innohub through SWRL rules. These rules, using the built-in `swrlb:containsIgnoreCase`, match the technical specifications of the components (used as keywords) with the textual descriptions and notes related to the attacks and vulnerabilities. The threats identified are then assigned to the `Threat` class, from which further subclasses can be derived, refining the search using parameters such as attack domain, typical severity, probability, or the likelihood of a more severe threat following an existing one.

The vulnerabilities present in the CVE-NIST database are associated with the list of hardware and software products in the CPE-NIST (Common Platform Enumerations) list. Once the list of hardware and software to be used in the Secured project is defined, each component can be accurately mapped to the CVE list, and consequently to the weaknesses and attack patterns in CWE and CAPEC.