7SHIELD

KR02 – Secure Authentication Mechanism

Purpose

7SHIELD is proposing an innovative **Secure Authentication Mechanism** ensuring secure personal data storage, secure encrypted personal data search, expressive and advanced access control over encrypted data and secure data integrity verification. The Secure Authentication Mechanism uses a hybrid encryption mode that elegantly merges symmetric encryption, attribute-based encryption, proxy re-encryption and searchable encryption.

Moreover, the Secure Authentication Mechanism ensures **confidentiality, integrity, availability** of transmitting protected information from falsification or modification and provides the user with **alternative passwordless authentication methods** (through the usage of hardware components in the form of secure elements, such as smart cards and SIM cards, as well as social logins).

Scope

The Secure Authentication Mechanism is designed to meet the requirements useful to develop TRL 7 **Prevention and preparedness tools** and **enables the detection and auto-mitigation against brute force attacks**.

The Secure Authentication Mechanism is being used by all the 7SHIELD modules which require user authentication and the integration with other 7SHIELD detection modules provides an additional robustness layer in case of unavailability. Moreover, its scalable deployment and the adoption of the standard **OpenID connect** protocol guarantees further applications in multiple contexts.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284

Prevention

Decision Support Systems

Partners

Serco Italia, CS GROUP and Exalens collaborated for the design and development of the secure authentication mechanism.

SERCO
Italy

Serco Italia is specialized in the Earth Observation and owns ONDA Data and Information Access Service (DIAS), a cloud platform enabling the exploitation of the Earth Observation data by allowing users to adopt, build or enhance applications and services.

CS GROUP
France

CS Group provides engineering services in ground segment platform for space and its applications market, and brings its technical expertise to specify an innovative solution for satellite data authentication, integrity, and confidentiality.

Exalens
Netherlands

Exalens has developed authentication services and identity management mechanisms in other H2020 projects.

All the modules developed in the frame of 7SHIELD have been designed with the consultancy of identified external stakeholders, first responders and following the **requirements** provided by the partners working in the space sector acting as Pilots, who provided the Critical Infrastructures for **testing and demonstration**.

Contribution

Serco Italia leads the design and development of the Secure authentication mechanism, providing expertise in the field of Data access in the space sector, ensuring the applicability of **GDPR** legislation and providing the infrastructure, hosted by the OVH **cloud provider**.

CS Group developed a **modular, scalable and reliable** (K8S) platform to host the authentication services and a **distributed ledger database (blockchain)** to ensure immutability of authentication data

Exalens developed **multi factor authentication** service and enabled the **social login** into the Secure authentication mechanism.

Stakeholders

Both **private and public companies distributing their data and services** might be interested in adopting the Secure Authentication Mechanism leveraging its **Single Sign-On** (SSO) function which **improves security, usability and infrastructure maintenance** while improving the **end user's convenience and trust**; Secure Authentication Mechanism ensures also the data integrity and the applicability of GDPR regulation.

Furthermore, the Secure Authentication Mechanism offers the possibility to remove some authentication vulnerability associated to the password because, in addition to the usual the password policies and forgot password mechanisms, it implements multi factor authentication and social login.

Contact

- adrianagrazia.castriotta@serco.com

Technology

The Secure authentication mechanism uses a cloud-based Identity, Access Management mechanisms and, in terms of operability, a container-based microservices architecture – **Kubernetes clusters orchestration** – guarantees the high availability of the authentication and authorization service.

The usage of **open-source software** for proxy reversing, ingress controlling, simple authentication, monitoring, alerting and route notification (such as **Apisix, Keycloak, Graylog Prometheus and Postfix**) reduce the maintenance and ensure a longest sustainability of the module.

Hyperledger database is the technology used for storing and transmitting information without central control entity while the multi factor authentication mechanism follows the **FIDO alliance standards**.

Future Improvements

The Secure authentication mechanism can be further improved with the support of the **Passkeys** which is a user authentication standard by the FIDO alliance. A Passkey is A FIDO Authentication credential that provides passwordless sign-ins to online services. The Passkeys are supported by all members of the FIDO alliance. With the adoption of the Passkeys, the Secure authentication mechanism can operate without the need of passwords, since passwords are one the main targets of threat actors.

www.7shield.eu