Identity and Access Management for Immersive Ecosystems
IMMERSE

Introduction

Immersive telepresence applications introduce novel challenges in identity management, privacy, and access control, as traditional approaches such as passwords are not well suited for these highly interactive and context-aware environments.

The IMMERSE integrates advanced identity and access management mechanisms into the SPIRIT platform through the use of Verifiable Credentials (VCs). To ensure both security and user trust, IMMERSE implements a **cloud-based wallet** built on top of SPIRIT's **Confidential Computing infrastructure**, enabling privacy-preserving credential storage, selective disclosure, and secure user authentication.

Objectives

- Enable real-time, user-centric, secure and privacy preserving authorization system for immersive systems
- Achieve compatibility with emerging Identity standards and new EU Digital Identity regulation
- Provide scalable, flexible, cloud-based deployment options

Key Features

Availability, interoperability, privacy, and security are the main considerations in the design of the IMMERSE ecosystem. The cVM, where the wallet is hosted, ensures **private keys, credentials**, and cryptographic operations are **isolated from the host**, the hypervisor and other tenants, and sensitive data is only stored in the encrypted memory of the Trusted Execution Environment (TEE). Additionally, all system components, including the issuer and the verifier, are implemented as containerized microservices and orchestrated using Kubernetes.

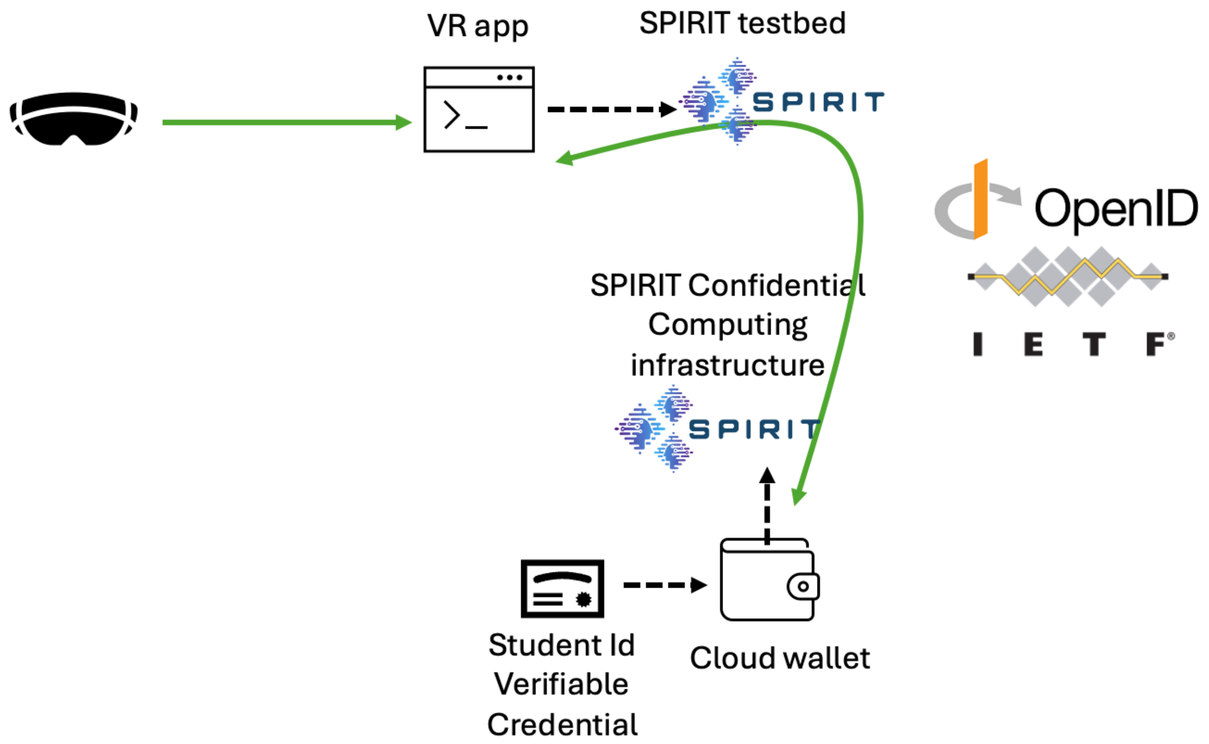

Fig.1: IMMERSE Overview

Architecture Overview & Testbed Setup

IMMERSE is developing a secure, **cloud-based VC wallet**, which is executed on a **confidential VM (cVM),** specifically AMD SEV, hosted in the **Deutsche Telekom 5G Standalone (SA)** testbed in Berlin. The wallet will interact with **immersive XR applications** hosted on the SPIRIT platform, by verifying user credentials through encrypted, cloud-hosted infrastructure, orchestrated via Kubernetes

We consider a simple use case scenario, namely, a virtual classroom rendered in a telepresence environment hosted by SPIRIT. A student uses XR equipment to join a course session. During onboarding, the IMMERSE wallet running inside a cVM, generates a Verifiable Presentation (VP) on behalf of the student, to prove course enrolment. The Verifier verifies the VP in real-time. Unlike traditional login flows that may force users to switch devices or remove their XR headset, our approach ensures that all identity-related interactions to join sessions in XR environments, are handled seamlessly within the immersive environment.

Conclusions and impact

IMMERSE introduces a secure and standards-based approach to identity management in XR environments, without interrupting the user experience. By combining cVMs with widely accepted standards and Kubernetes orchestration, we isolate sensitive operations and data, while ensuring availability and flexibility. With Kubernetes and Helm, the system remains portable and scalable, as it can be deployed across different setups, from testbeds to production environments, and is an identity management solution compatible with most XR use cases.

References

- OpenID Foundation. (2022). **OpenID for Verifiable Credential Issuance (OID4VCI).**
- OpenID Foundation. (2022). **OpenID for Verifiable Presentations (OID4VP).**
- World Wide Web Consortium (W3C). (2019). **Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web.**
- Stephenson, S., Pal, B., Fan, S., Fernandes, E., Zhao, Y., & Chatterjee, R. (2022). **SoK: Authentication in Augmented and Virtual Reality**. 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 267-284.
- George, C., Khamis, M., von Zezschwitz, E., Burger, M., Schmidt, H., Alt, F., & Hussmann, H. (2017, February). **Seamless and secure VR: Adapting and evaluating established authentication systems for virtual reality**. NDSS.

Contact

Nikos Fotiou
ExcID
fotiou@excid.io

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra. Swiss Confederation. Federal Department of Economic Affairs, Education and Research EAER. State Secretariat for Education, Research and Innovation SERI
UK Research and Innovation