Digital Services Integration in Smart Cities: a Trusted Execution Environment Based Solution *

Regis Schuch[1], Rafael Z. Frantz[1], José Bocanegra[2], Fabricia Roos-Frantz[1], Sandro Sawicki[1], Carlos Molina-Jiménez[3]

[1]Unijuí University – Ijuí – Brazil

[2]University of los Andes – Bogotá – Colombia

[3]University of Cambridge – Cambridge – United Kingdom

{regis.schuch, rzfrantz, frfrantz, sawicki}@unijui.edu.br,

j.bocanegra@uniandes.edu.co, carlos.molina@cl.cam.ac.uk

Abstract. *This paper elucidates the use of Trusted Execution Environments as a solution to the challenges of data security and privacy within the context of digital services integration in smart cities. This type of environment is engineered to safeguard sensitive data during execution, thereby guaranteeing that tasks involving such data are performed within isolated memory compartments.*

Keywords*: Privacy. Morello Board. Compartmentalisation.*

A smart city integrates physical, IT, social, and business infrastructures, utilising collective intelligence [Harrison et al. 2010]. To be considered smart, cities must develop three dimensions: people, institutions, and technologies [Nam and Pardo 2011]. This paper focuses on the technological dimension, which includes a rich ecosystem of digital services from both the public and private sectors. These services must be interoperable and integrated to provide new services, thereby supporting business processes. Integration platforms are specialised software tools used to design, implement, and run integration processes. An integration process is designed as a workflow of tasks that implements an integration logic, allowing two or more digital services to exchange data and share functionality. Data that flows within the integration process must be protected against external and unauthorised access, thereby preventing data leaks and preserving privacy.

To circumvent these issues, we propose a hardware-based approach that utilises a TEE to execute the integration process. A TEE is a secure environment within a processor capable of executing code containing confidential data [Sabt et al. 2015]. In our proposal, we have chosen to use the Morello Board [ARM 2022] TEE implementation, as it incorporates Capability Hardware Enhanced RISC Instructions (CHERI) concepts [Watson et al. 2019], enabling fine-grained memory protection. A distinguishing feature of the Morello Board is that a developer can control specific areas in the memory, which is not possible with other TEE implementations on the market. Morello's software ecosystem is compatible with operating systems such as

*Supported by the Coordination for the Improvement of Higher Education Personnel (CAPES) and the Brazilian National Council for Scientific and Technological Development (CNPq) under the following project grants 309425/2023-9, 402915/2023-2, 311011/2022-5.

CheriBSD [Watson and Davis 2023], which incorporates specific features of the CHERI architecture. Library compartmentalisation allows each library to operate in its own protection domain within a compartmentalisation-enabled process [Watson et al. 2023].

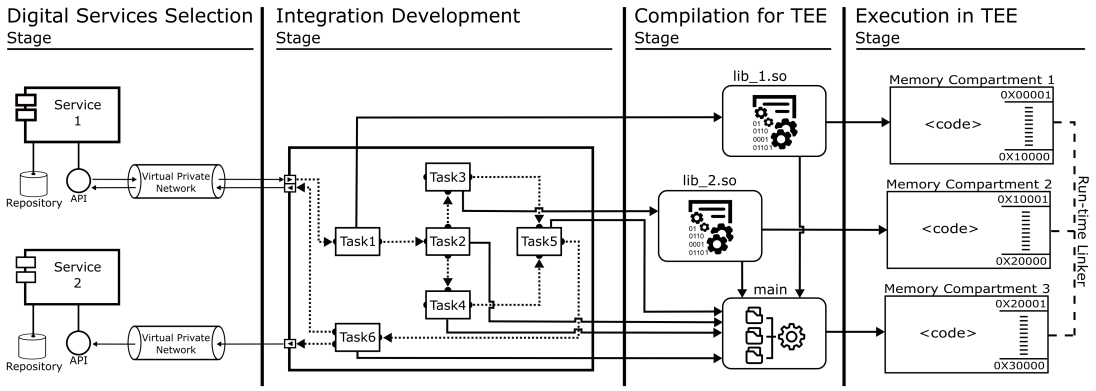

Figure 1. Stages for executing an integration process in a TEE.

Roughly speaking, we divide the process of executing an integration process in a TEE into four stages as illustrated in Figure 1. Digital Services Selection entails analysing data repositories to identify available data, access methods, and protocols, and ensuring data transmission through secure channels like Virtual Private Network (VPN). Integration Development involves creating processes and atomic tasks for data operations. Compilation for TEE involves implementing integration process components as libraries, and deployment in a secure environment requires compilation in CheriBSD. Finally, objects are executed in TEE instantiated in the Morello Board, accessing memory spaces and the run-time linker. The run-time linking process creates compartments for each library, granting and restricting access to resources, and communication between compartments occurs through function calls and passing arguments. We implemented and experimented with this strategy and our view is that it is viable in practice, as it allows for the protection of data flowing through an integration process.

References

ARM (2022). Morello prototype architecture. `https://developer.arm.com/documentation/den0133/0100/?lang=en`. [online: access in 10-jan-2024].

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., and Williams, P. (2010). Foundations for smarter cities. *IBM J. of R. and Dev.*, 54(4):1–16.

Nam, T. and Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proc. 12th Annual Int'l Digital Government Research Conf.: Digital Government Innovation in Challenging Times*, page 282–291.

Sabt, M., Achemlal, M., and Bouabdallah, A. (2015). Trusted execution environment: what it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/Ispa*, pages 57–64.

Watson, R. N., Moore, S. W., Sewell, P., and Neumann, P. G. (2019). An introduction to cheri. Technical report, University of Cambridge, Computer Laboratory.

Watson, R. N. M. and Davis, B. (2023). Getting started with cheribsd 23.11. `https://ctsrd-cheri.github.io/cheribsd-getting-started/cover/index.html`. [online: access in 11-jan-2024].

Watson, R. N. M., Witaszczyk, K., and Man, J. (2023). Library compartmentalization. `https://www.cheribsd.org/tutorial/23.11/c18n/index.html`. [online: access in 11-jan-2024].