Navigating Security Issues of Interoperability in the Digital Identity System of a Smart City

Authors: Amarilda Koka, Pierre-Martin Tardif

The Thirteenth International Conference on Smart Cities, Systems, Devices and Technologies
SMART 2024

Presenter: Amarilda Koka - Student, CYBERUS- Erasmus Mundus Joint Master Program
Email: koka1501@usherbrooke.ca

Amarilda Koka

Amarilda Koka received the Bachelor diploma in Business Informatics at University of Tirana, Albania 2021. During her undergraduate studies, she established her first startup, completed several internships in the field of technology and finance, and was an active student in several training in Information Security.

She is currently a master student in Cybersecurity at University of Luxembourg as part of the CYBERUS Erasmus Mundus Joint Master program, where she is currently doing an internship in Information and Cybersecurity in satellite communication industry.

The research internship at the University of Sherbrooke, Canada, significantly motivated her to delve deeper into the subject matter.

Aims and contributions of our paper

Safeguard user privacy and maintain effective interoperability between varied platforms.

Explores the barriers to seamless interoperability among various digital identity systems.

Identify security attacks in digital identity system.

Contribution: Demonstrate an innovative approach designed to meet the significant security attacks in digital identity system.

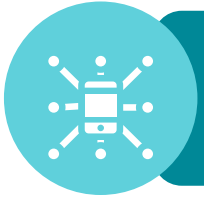
Key Concepts and Definitions

Digital Identity

Digital identity in Smart Cities securely verifies individuals' access to urban services, enhancing efficiency and trust.

Interoperability

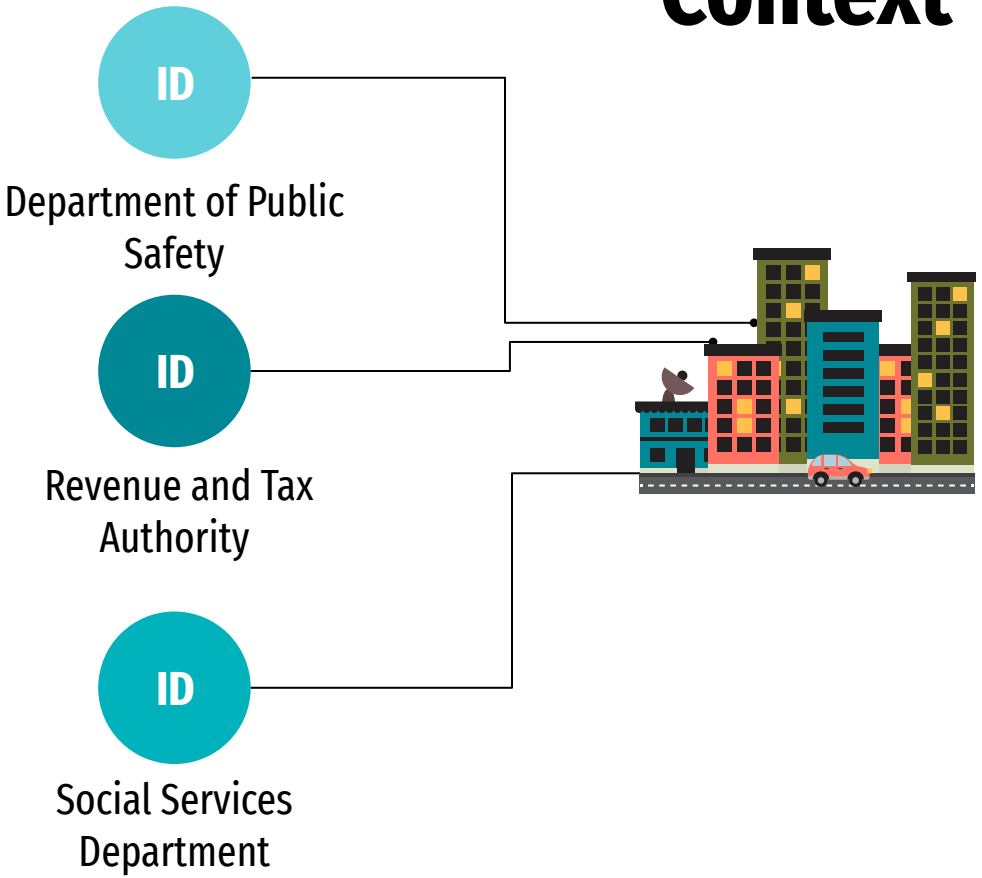
The ability of Information and Communication Technology (ICT) systems and the business processes they support to exchange data and enable the sharing of information and knowledge.



PCTF

The Pan-Canadian Trust Framework plays a pivotal role in setting the standards to secure digital identity landscape across Canada.

Context



Use of electronic identity management to improve collaboration between government agencies by reducing duplication of efforts and increasing the efficiency and effectiveness of resource utilization.

Interoperability Challenges

01

Lack of communication across jurisdictions

Government services perceived as a unified entity by the public require interactions with multiple departments, leading to communication barriers and fragmented service delivery.

02

Security risks

Data breaches or leaks present substantial correction challenges, heavily dependent on existing protocols and their implementation.

03

International collaboration and standardization challenges

Efforts between countries (e.g., Canada and the European Commission) highlight the need for international cooperation to address digital identity interoperability.

04

Emerging technologies and regulatory compliance

Determining whether ZKP proofs constitute personal data requires careful consideration to align with privacy regulations.

Security Issues

Security Attacks on IAM Technologies

1

307 Redirect Attack in OAuth

Attackers exploit incorrect HTTP redirection status codes at the Identity Provider (IdP) level.
This error during the redirection process compromises authorization and authentication, potentially exposing user credentials during login.

2

Man-in-the-Middle (MITM) Attack in SAML

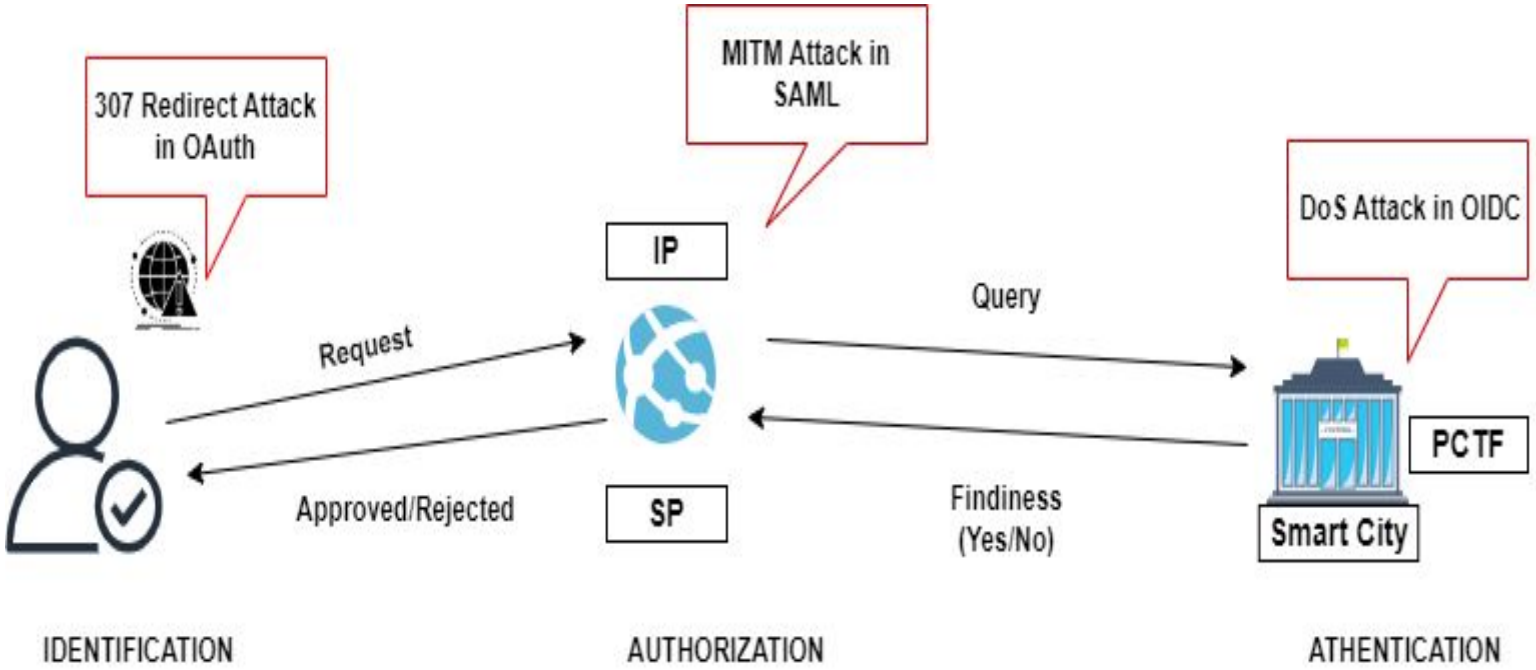
Attackers can intercept or alter communications between the user and the Service Provider (SP), especially where SOAP binding is used without adequate security measures like digital signatures on assertions, increasing the risk of identity theft or unauthorized access.

3

Denial-of-Service (DoS) Attack in OpenID Connect (OIDC)

Potential for DoS attacks during the OIDC identity provider's configuration information discovery process.
Publicly accessible metadata endpoints can be overwhelmed with requests, impacting the availability of the OIDC service and disrupting legitimate user access.

Smart City- Digital Identity System Model



USE CASE: SEAMLESS USER AUTHENTICATION IN THE DIGITAL IDENTITY INTEROPERABILITY MODEL FOR SMART CITIES

1

Identification

Alice seeks to access a service. She provides her current identifiers to the respective Service Providers she engages with.

2

Role of the Smart City

Is the intermediary account holder. It does not store or process of user information.

3

Authentication Request

The public transport service sends an authentication query to Smart City, seeking verification of Alice's student card.

5

Authentication Outcome

The university provides a minimal response, confirming Alice's student status "Yes" or denying it as "Not".

6

Authorization

The Service Provider proceeds to grant access to the user's account based on the authentication outcome.

7

SecureID

This approach ensures enhanced privacy, trust, and security in the digital identity ecosystem.

Conclusion

- The current situation, as demonstrated by the Canadian Federation's decentralized identity management systems, emphasizes the necessity for a single and dependable identification system.
- As digital identity management evolves, the research emphasizes the need for seamless interoperability, which presents a range of challenges including data exchange, authentication compatibility, privacy management, and regulatory compliance.
- To address these issues, a proposed system model for Smart Cities is presented, stressing the government's role as an intermediary account holder in allowing secure and transparent identification processes. The approach seeks to achieve a careful balance between resolving security issues and promoting frictionless data interchange, supported by collaboration, standardization, and strong security safeguards.
- The proposed approach is consistent with the principles of least privilege and segregation of roles, which contribute to a robust and user-friendly IAM cycle.

Future Work

- It is imperative to conduct in-depth investigations into the implementation and practical viability of Zero-Knowledge Proofs (ZKP) for secure identification, ensuring that user data remains confidential while enabling seamless verification across platforms.
- As quantum computing advances, comprehensive studies are warranted to explore and adopt quantum-safe encryption techniques, such as lattice-based encryption and hash-based signatures, to fortify digital identity systems against potential quantum threats.
- More research focus needed on developing fault-tolerant frameworks that enable automated recovery from transaction failures, enhancing the overall reliability and continuity of the system.
- Regulatory and governance bodies must actively reassess existing policies to accommodate decentralized identity (DID) and Self-Sovereign Identity (SSI) approaches while upholding data protection principles.
- Empowering users with comprehensive knowledge of digital identity concepts and privacy rights through educational initiatives will foster trust and confidence in the system.

References

[1] DIACC/CCIAN. Digital ID for Canadians. https://diacc.ca/, 2024. [Online; accessed 2024-03-22].

[2] M. Lips and J. A. Taylor. Economic and Social Research Council (Great Britain). Personal identification and identity management in new modes of e-government, 2007. Swindon: Economic & Social Research Council.

[3] Anuja Sharma, Sarita Dave, and Meenu. Identity and access management-a comprehensive study. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), pages 1481 1485. IEEE, 2015.

[4] Anuja Sharma, Sarita Dave, and Meenu. Identity and access management-a comprehensive study. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), page 1482. IEEE, 2015.

[5] Sirapat Boonkrong. Authentication and access control: practical cryptography methods and tools. Springer, 2021.

[6] J. Bonneau et al. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy, pages 553–567. IEEE, 2012.

[7] I. Georgiou et al. Blockchain for smart cities: a systematic literature review. In Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, November 25–26, 2020, Proceedings 17, pages 169–187. Springer, 2020.

[8] Official Publications of the European Communities. European Interoperability Framework for Pan-European eGovernment Ser vices. https://op.europa.eu/en/publication-detail/-/publication/a4778634 27fa-43b4-9912-f753c4fdfc3f, 2004. [Online; accessed 2024-03-22].

References

[9] e-Government Interoperability: Overview. Report, United Nations Development Programme (UNDP), 2007.
[10] Canada-EU Joint Workshop Series for Enabling Interoperability and Mutual Support for Digital Credentials. https://digitalstrategy.ec.europa.eu/en/library/canada-eu-joint-workshop-series enabling-interoperability-and-mutual-support-digital-credentials, 2021. Workshop series conducted by [Organizing Body/Institution], [Location, if available].
[11] E. Damiani et al. Managing multiple and dependable identities. IEEE Internet Computing, 7(6):29–37, 2003.
[12] F. Paci et al. An interoperable approach to multifactor identity verification. Computer, 42(5):50–57, 2009.
[13] D. Fett et al. A comprehensive formal security analysis of OAuth 2.0. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 1204–1215. ACM, 2016.
[14] T. Logerstedt et al. OAuth 2.0 threat model and security considerations. Technical report, 2013.
[15] J. Somorovsky et al. On breaking {SAML}: Be whoever you want to be. In 21st USENIX Security Symposium (USENIX Security 12), pages 397–412. USENIX, 2012. [16] A. Armando et al. An authentication flaw in browser-based single sign on protocols: Impact and remediations. Computers & Security, 33:41 58, 2013.
[17] Thomas Groß. Security analysis of the SAML single sign-on browser/artifact profile. In 19th Annual Computer Security Applications Conference, 2003. Proceedings., pages 298–307. IEEE, 2003.
[18] R. Vaughn et al. Information assurance measures and metrics-state of practice and proposed taxonomy. In 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the, pages 10–pp. IEEE, 2003.

THANK YOU!