Contribution ID: **17** Type: **Talk**

Data driven analysis of National Public Key Infrastructure frameworks across cybersecurity-leading countries.

Public key infrastructure (PKI) is a key component of modern information technology (ICT) infrastructures, particularly in South Africa. In this study, we aim to identify the components and models of NPKI from countries with strong cybersecurity postures and examine the effect of policy and regulatory environments for PKI development.

The study employed a phenomenological approach to gather data aimed at comprehending the existing developments in PKI frameworks, thereby recommending step by step development of a theoretical framework that can be applicable to the country. Data were collected from government reports, peer-reviewed journals, books, conference papers and websites, published between 2015 and 2025.

In addition, literature studies were reviewed to obtain the recommended list of those countries with good cybersecurity posture. The results indicated that the domain of information security, particularly public key infrastructure, has experienced substantial transformations and is anticipated to encounter further developments in the future. Additionally, leveraging cloud-based PKI services for scalability and cost-effectiveness, ensuring compliance with global security standards, and implementing decentralized PKI to mitigate risks associated with central points of failure. Developing a comprehensive, quantum-safe PKI that aligns with digital strategies and national ICT infrastructures is important for enhancing security and cost effectiveness, especially in countries like South Africa, especially for large-scale sectors like E-government and E-commerce.

Primary authors: Mr COSSA, Bheki; Ms KHUMALO, Lethukuthula

Co-author: Mrs NTSHANGASE, Sthembile (Software Engineer)

Presenters: Mr COSSA, Bheki; Ms KHUMALO, Lethukuthula