



Shared Prosperity Dignified Life



Workshop on Building Trust in Digital Government Services

Organized by ESCWA in collaboration with AICTO, Internet Society, and ITU.

Beirut, 11-12 September 2023 (and via Zoom)

Preliminary Information Note

Background

Governments globally, including Arab nations, have been actively pursuing public sector digitization for over two decades. The COVID-19 pandemic has accelerated the urgency for digital transformation and efficient online service delivery. However, for this transformation to be successful, it is paramount to establish and maintain trust and confidence among citizens and stakeholders. Digital transformation holds significant potential for facilitating the access to government services, improving effectiveness of public sector, enhancing governance, citizen participation, and engagement in decision-making processes.

Today the emerging technologies such as artificial intelligence, big data, and Internet of Things are spreading, and they present both opportunities and challenges. While these technologies can strengthen cybersecurity and improve digital government services, they also introduce risks. Inadequate management of these technologies can compromise cybersecurity measures, compromise data privacy, hinder data sharing, and potentially impact citizens' well-being. It is, thus, imperative to gain a comprehensive understanding of these technologies and develop effective strategies and measures to harness their positive impact on trust in digital services and government.

ESCWA has recently launched a project on "Expediting the use of technology and innovation for enhanced operations in Arab public institutions" (ENACT). The project focuses on the innovative deployment of emerging technologies to accelerate the implementation of adopted digital strategies and to establish responsive, inclusive, trustworthy, and effective governments in support of the 2030 Development Agenda, particularly SDG 16 on peace, justice, and strong institutions.

Digital Trust is a paramount concern for the Arab Information and Communication Technologies Organization - AICTO, which is dedicated to leveraging its wealth of experience and expertise to actively contribute to global endeavours aimed at fostering collaboration. The primary objective is to cultivate robust and reliable digital economies within the Arab region, thereby enhancing the well-being of Arab citizens through the utilization of digital services. As part of this overarching goal, AICTO initiated the "AAECAET" project, also known as the "Interregional Digital Trust Network," in 2017. This project serves as a comprehensive framework that brings together various stakeholders to promote interoperability, mutual recognition, and harmonization of laws on digital trust services.

In the realm of cybersecurity, AICTO has embarked on an extensive journey of capacity building activities. In 2022, AICTO introduced the "Arab Cybersecurity Strategy" with a visionary objective of creating a secure, safe, and inclusive Arab society that seamlessly integrates into the global digital economy. The strategy emphasizes the empowerment of self-reliant solutions and expertise, with a strong focus on bolstering digital confidence and trust within the Arab cyberspace. By doing so, AICTO aims to ensure the stability and integrity of the digital landscape in the Arab region.

As Arab states modernize and diversify their economies, focusing on digital services, e-commerce, and e-government, the importance of ensuring continuous internet connectivity becomes crucial. This requires prioritizing cybersecurity and implementing policies, technologies, and best practices that strengthen

internet infrastructure security. Contemporary cybersecurity frameworks recognize that security is integral to broader social and economic goals, supporting an interconnected global digital economy. Collaboration and partnerships are key to achieving this. Guided by regional experts, and international and regional frameworks on cybersecurity, the Internet Society has identified the essential principles to secure the Internet in its “Internet Infrastructure Security Guidelines for the Arab States”.

Encryption is vital in safeguarding personal and national security. It protects private messages, online banking, air traffic control, medical data, and e-voting, shielding online information from eavesdropping and tampering. Preserving encryption requires collective efforts to educate policymakers about proposals that may compromise online security. Governments, as major data repositories, face significant cyber threats. Data breaches have exposed voter records, digital identities, and classified state secrets. Safeguarding government systems requires robust measures and constant vigilance. To support government decision makers and citizen for understanding well the encryption process, ISOC has developed a specific course on Encryption.

A fundamental role of the ITU, based on the guidance of the World Summit on the Information Society (WSIS) and the ITU Plenipotentiary Conference, is to build confidence and security in the use of Information and Communication Technologies (ICTs). The ITU cybersecurity programme offers member states – particularly developing countries – the opportunity and tools to increase cybersecurity capabilities, to enhance security, build confidence and trust in the use of ICTs – making the digital realm more safe and secure for everyone. This includes the ITU Global Cybersecurity Agenda (GCA), a Guide to developing a national cybersecurity strategy, the Global Cybersecurity Index (GCI) and assistance and workshops for enhancing National Computer Incident Response Teams (CIRTs) in Arab countries.

Objectives

The workshop will analyse and build on existing frameworks for cyber security at the international and regional levels, as well as advances made in many Arab countries in cyber security, development of digital government, and automation of internal government process.

The main objective of this workshop is to showcase practical strategies for enhancing cybersecurity, discuss best practices on the use of emerging technologies for improving trust and confidence in digital government services and argues on how to enhance privacy and personal data protection for the delivery of trusted digital services. The workshop will also discuss the new trends for mutual recognition of trusted services in the Arab region.

The workshop would primarily showcase experiences from developed and developing countries, including Arab countries. Initiatives and projects from international and regional organizations that assist developing countries in the aforementioned areas will also be evaluated.

The workshop brings together stakeholders from government entities, cybersecurity experts, policy makers, and industry professionals to discuss available strategies and guidelines, and to present practical measures to enhance trust in digital public services.

Expected Outcomes

The main outcome of this workshop will be a set of practical and actionable recommendations that will enhance cybersecurity and foster trust in digital government services across the Arab region. In addition, the workshop will highlight best practices from both developed and developing countries that can serve as guidance for other nations.

These recommendations will primarily target governments, regulatory authorities, and institutions involved in ICT and technology implementation in government operations. Drawing from successful practices and measures, the workshop will identify practical steps and emerging technology trends that can contribute to the creation of a secure cyberspace and reliable digital services.

The workshop's outcomes will be incorporated into the main report of the ESCWA ENACT project, titled "Policies and Best Practices for Leveraging Technology and Innovation in the Advancement of Arab Public Institutions".

Organization, Participation and Registration

The workshop is organized by ESCWA in partnership with the [Arab ICT Organization](#), the [Internet Society](#) and the [International Telecommunications Union](#). It is a hybrid event and will take place at the UN-House in Beirut, from 11 to 12 September 2023, and through Zoom. It will be conducted in both Arabic and English, with simultaneous interpretation.

Officials from ministries and public agencies working in ICT, digital government, cybersecurity, and administrative development are among those invited. Experts from the United Nations, international and regional organizations, academia and non-governmental organizations will also be invited.

Please visit <https://indico.un.org/e/trust-digital-services> to register for the event. More details, including workshop documents, can be found on the event page at <https://www.unescwa.org/events/building-trust-digital-government-services>

Discussion Topics

During the workshop, the following topics will be discussed:

- Understanding the importance of trust and confidence in digital government services.
- Emerging technologies for enhancing security and trust in cyberspace and digital services.
- Privacy and personal data protection for trusted digital government services.
- Internet Infrastructure Security Guidelines for the Arab States
- Encryption as important instrument for enhancing cybersecurity and trust in digital services.
- Arab Cybersecurity Strategy with focus on indicators and indexes, compliance with the international standards, legal measures, enhancing the maturity of institutional and administrative structure).
- Building Digital Trust: Reality and Prospects for the Arab region.

Focal Points

Economic Social Commission for Western Asia - ESCWA

Ms. Nibal Idlebi
Acting Director of Statistics, Information Society and Technology Cluster
E-mail: idlebi@un.org

Administrative inquiries can be sent to:
Ms. Khadija Mansour, Administrative Assistant
E-mail: mansour10@un.org

Arab Information and Communication Technologies Organization - AICTO

Ms. Nada Laabidi
Head of Planning and Projects Department
Email: n.laabidi@aicto.org

Internet Society - ISOC

Ms. Nermine El Saadany
Regional Vice President for the Middle East
Email: Saadany@isoc.org

International Telecommunications Union – ITU

Mr. Ahmed El Raghy
Senior Advisor
Email: Ahmed.ElRaghy@itu.int