Progress of Taiwan PKI

Chinese Taipei PKI & e-Authentication Consortium
Clement Hsieh, Senior Engineer, ITRI

May 8, 2023

Outline

- **Establishment of Ministry of Digital Affairs (moda) in Taiwan**
- **Government's introduction and promotion of zero-trust network architecture**
- **Progress Update**
  - **PKI & FIDO**
  - **Electronic Signature**

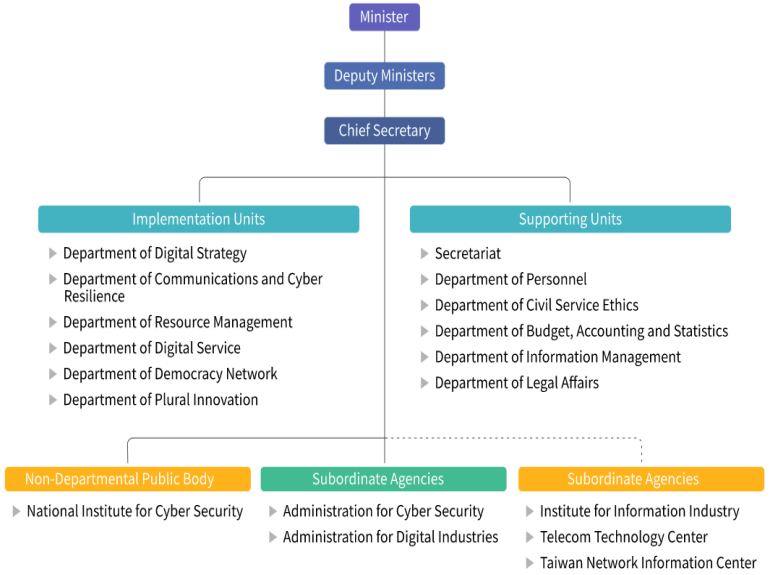
Establishment of Ministry of Digital Affairs (moda) in Taiwan (1/4)

Background

- **In the era of 5G and IoT (Internet-of-Things), digital technology is changing our ways of life and reshaping the ecosystem of industries.**
- **The Ministry of Digital Affairs (moda) was established to keep up with the mega trend in technology, pointed out by President Tsai Ing-wen indicated in 2019.**
- **The recently established moda seeks to integrate the government agencies in information, networking and communication in a groundbreaking manner and assist the Taiwanese society in digital transformation.**

Establishment of Ministry of Digital Affairs (moda) in Taiwan (2/4)

- The establishment of the Ministry of Digital Affairs (moda) on August 27, 2022, after a long period of preparation marks an important milestone in digital development of Taiwan
- The abbreviation "moda" indicates the Ministry of Digital Affairs' aspiration to serve as a "motor" in digital development of Taiwan
- The "moda" endeavor to create digital resilience of the public by connecting people with technology, promoting industries and safety and accelerating the digital development of the society to realize the vision of a smart state
- The "moda" has become the competent authority of the "Electronic Signature Law" , and
  - is planning the revision of the law
  - continue to support the CTPKIC and APKIC



Source: moda

Establishment of Ministry of Digital Affairs (moda) in Taiwan (3/4)

Major Policies

- **Drive the national digital development strategy and coordinate the planning of project resources**
- **Deploy the key infrastructure in communication and enhance the resilience of communication networks**
- **Allocate and manage digital communication resources in a forward-looking manner to ensure resource utilization meets public interest**
- **Strengthen digital applications and boost government efficacy**
- **Participate in the international digital network of democracy and contribute more to the international society**
- **Develop data use cases and create the digital ecosystem of public interest**

Establishment of Ministry of Digital Affairs (moda) in Taiwan (4/4)

Major Policies

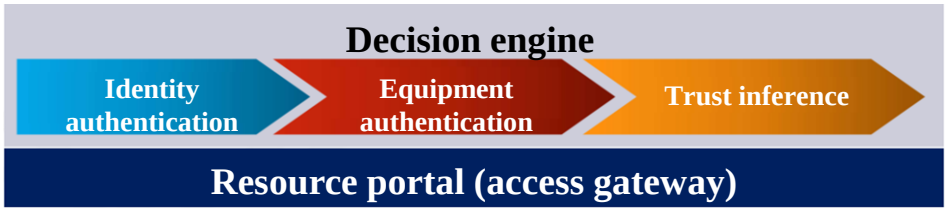
- **Accelerate digital industrial innovation and transformation and promote the development of digital related industries**
- **Strengthen cybersecurity and defence-in-depth and enhance the resilience of the national digital development environment**

Opening ceremony and minister appointment

Minister Audrey Tang presents online at Asia Pacific Regional Internet Governance Forum (APrIGF) to share about how Taiwan's digital transformation helps in carbon reduction

Government's introduction and promotion of zero-trust network architecture (1/2)

- Taiwan government introduces and promotes the zero-trust network architecture according to the national information and communication security development program (2021-2024).
- Taiwan's zero-trust network architecture is established in reference to Special Publication 800-207: Zero Trust Architecture (ZTA) released by the National Institute of Standards and Technology (NIST) of the U.S.
- The resource portal-based deployment allows only access via access gateways for both internal and external users
- Network connections between users and information and communication systems of organizations are established, monitored and terminated based on decisions by the decision engine, which consists of three core mechanisms: identity identification, equipment identification and trust inference.



Source:
National Center for Cyber Security Technology (NCCST)

Government's introduction and promotion of zero-trust network architecture (2/2)

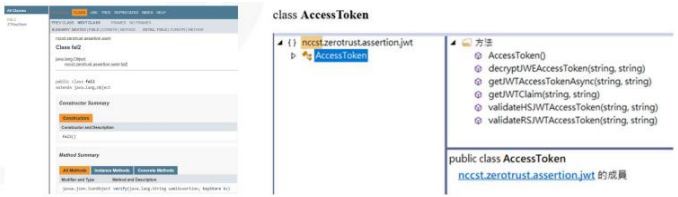
- Identity identification is the mechanism prioritized for introduction of the zero-trust network. This includes the following:

  - ☐ Multi-factor identity identification

    Such as FIDO (Fast IDentity Online) and use USB tokens or mobile apps to login without passwords

  - ☐ Identity identification declarations with e-signatures and encryptions

After users have obtained access tokens, the identity declaration server issues users the certificate of authorized access (e.g., JWT and SAML). Identification validation declaration can be obtained by connecting to the identification declaration API of the information and communication systems of organizations.



Source: NCCST

Update of PKI & FIDO(1/2)

- Integration of TW FidO App and Citizen Certificate for more convenient and efficient identification and digital signing (Ministry of Interior, MOI)
  - The current Citizen Certificate is a physical card. It is necessary to use a computer and a card reader and unlock the card with passwords/PIN code
  - The new "Mobile Citizen Certificate" integrated the Citizen Certificate and TW FidO App. Biometric authentication is used instead of passwords/PIN code.
  - Easy access to government services (e.g., tax filing, COVID-19 health certificate application, online voting of shareholders, signing of official document, etc.)
  - Expansion of use cases by allowing telecom operators and financial institutions to leverage the "Mobile Citizen Certificate"

Source: Ministry of the Interior, Ministry of Digital Affairs

Update of PKI & FIDO(2/2)

- Minister of Digital Affairs had **joined International FIDO Alliance in Feb., 2023**
  - As authentication and electronic signatures are both key issues in secure online transactional environments, after its launch in August, the MODA has been actively discussing how to react accordingly to rapidly evolving digital technology and how to build a more complete environment as a foundation for **digital trust**.

	Verification	Authentication	AuthoZ/eSign
Possible Application	Web Retail Shopping	Retail, Telecomm	Fintech/SupplyChain
Descriptions	Internet shopping or social platform that requires the actual identity registration.	Using FIDO and credentials for trust services online.	B2B transactions that requires secure and non-reliable confirmation in supply chain and between institutions
Association	中華民國無店面零售商業同業公會 Chinese Non-Store Retailer Association; TTIDA 台灣電信產業發展協會; 中華金融科技產業促進會 FinTech Industry Development Association; 臺灣金融科技協會		
Government	moda 數位發展部	內政部	金融監督管理委員會 Financial Supervisory Commission R.O.C. (Taiwan)

Source: Ministry of the Interior, Ministry of Digital Affairs

Update of eSignature (1/2)

Regulatory adjustments to the E-Signature Law

- In response to foreign chambers of commerce , MODA identified "E-Signature Technologies Recognized as Effective" explanatory letter in 2022/12/29
- List the specific technology and standards of e-signatures comply with Taiwan e-Signature regulations.

Trends	Providing
In practice, it is not easy to identify electronic signature comply with regulation	Related tech and standards list
Post Covid-19, electronic signature plays a more important role	Any open PKI standards - PKIX EU eIDAS AES and ETSI standards US NIST, ISO e-Sign algorithms

Source: Ministry of the Interior, Ministry of Digital Affairs

Update of eSignature (2/2)

Reg. Purpose	• Government plays key role • Remove limitation	• Moved to TSPs to operate	• Free market • Depending on tech providers	• Regional organization • Regulation and tech conformance
E-Sign layer types	2 layers – • e-Signature • Digital Signature	1 * Depending TSP	No regulated	3 layers – • SES • AES • QES

Regulatory Changes to the E-Signature Law

- Consider the **legal and evidence validity**
- Promote the **digital infrastructure** after post COVID-19
- Consider Certificate Authority **(CA)** organization and **Trust Service Provider (TSP)** management
- Consider **electronic documents + electronic signatures exchange** in the cross countries' scenarios

Source: ITRI and III researches

Asia PKI Consortium

THANK YOU