Electronic Commerce and Transaction Policy

Document Information

Title: Electronic Commerce and Transaction Policy

Policy Reference: TASMU-ETX-POL

Policy Number: 006/2020

Published Version: V1.0

Status of This Policy: FINAL DRAFT FOR PUBLICATION

Policy Abstract

This is the TASMU Electronic Commerce and Transaction Policy which provides the rules and regulations for all electronic commerce and transactions used within the TASMU Ecosystem, including the use of digital signatures, electronic commercial rules and payment services, related to those transactions.

Copyright Notice

Requirements Language

The key words “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as follows:

- **SHALL**: This word, means that the definition is an absolute requirement of the policy.
- **SHALL NOT**: This phrase, means that the definition is an absolute prohibition of the policy.
- **SHOULD**: This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase “NOT RECOMMENDED” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY**: This word, or the adjective “OPTIONAL”, mean that an item is truly optional.

Normative References

[Consumer Protection Law]

Law No. (8) of (2008) regarding Consumer Protection (the “Consumer Protection Law”), 2018, Ministry of Commerce and Industry (MOCI)

[Electronic Commerce and Transactions Law]

Decree Law No. (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law

[Electronic Signature Formats]

Electronic Signature Formats Standards, Qatar Public Key Infrastructure Section, Version 1.0, Aug 2018, MOTC

[ETSI EN 319 122]

Electronic Signatures and Infrastructures (ESI);CAdES digital signatures; ETSI EN 319 122-1, V1.1.1, April 2016, ETSI

[ETSI EN 319 132]

Electronic Signatures and Infrastructures (ESI);XAdES digital signatures; ETSI EN 319 132-1, V1.1.0, February 2016, ETSI

[ETSI EN 319 142]

Electronic Signatures and Infrastructures (ESI);PAdES digital signatures; ETSI EN 319 142-1 V1.1.0, February 2016, ETSI

[ETSI EN 319 411]

Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates; ETSI EN 319 411-1, V1.2.2, April 2018), ETSI

[ETSI SR 019 020]

The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments, ETSI SR 019 020, V1.1.2, October 2016, ETSI

[ETSI TS 119 101]

Electronic Signatures and Infrastructures (ESI);Policy and security requirements for applications for signature creation and signature validation, ETSI TS 119 101, V1.1.1, March 2016, ETSI

[PCI Data Security Standard]

Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2.1, May 2018

[TASMU Data Policy]

TASMU Experience Policy, 2020, TASMU

[TASMU Experience Policy]

TASMU Experience Policy, 2020, TASMU

[TASMU Security Policy]

TASMU Security Policy, 2020, MOTC

Informative References

[EU Directive on Digital Goods]

2019/770 EU Directive on certain aspects concerning contracts for the supply of digital content and digital services, May 2019, EU

[Mastercard Merchant Rules]

Mastercard Rules, Dec 2019, Mastercard

[Qatar's E-commerce Guidelines]

MOTC, Qatar's E-commerce Guidelines, April 2018

[Visa Core Rules]

Visa Core Rules and Visa Product and Service Rules

Contents

- Electronic Commerce and Transaction Policy
  - Document Information
  - Policy Abstract
  - Copyright Notice
  - Requirements Language
  - Normative References
  - Informative References
- Contents
- Definitions
- 1. Introduction
  - 1.1 TASMU
  - 1.2 Electronic Commerce & Transaction Policy
  - 1.3 Compliance
- 2. Electronic Commerce
  - 2.1 Service Operator Identification & Authenticity
  - 2.2 Service Operator E-Commerce Obligations
  - 2.3 Monetisation of Services
  - 2.4 Payments
- 3. Electronic Transactions
  - 3.1 Digital Signatures

Definitions

The definitions used in this policy have been written to provide contextual clarity and where necessary specificity, and should not be interpreted to be contradictory to any laws in the State of Qatar.

[Digital Signature]

Is an electronic signature, a cryptographic binding attachment or logical association with other data (to be signed) which is used by the Subscriber to indicate their approval on the data (to be signed).

[Electronic Transaction]

Any deal, contract or agreement concluded or performed, in whole or in part, through electronic communications.

[Internet of Things]

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, uniquely identified with the ability to transfer data over a network to Sector Platforms and/or the Central Platform.

[Personal Data]

Data of a natural person ('individual') which is specifically identifiable or can be reasonably identified either by the Personal Data itself or through a combination of other data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[Processing]

Any operation or set of operations which is performed on Personal Data, such as collecting; recording; organizing; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission, dissemination or otherwise making the data available; aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means.

[Signatory]

A person that has the legal right to access Signature Creation Information, and acts either on its own behalf or on behalf of the person it represents to use Signature Creation Information to create a Digital Signature.

[Signature Creation Information]

Refers to information, codes or private cryptographic keys used by the Signatory to create a Digital Signature.

[Subscriber]

An organisation or individual who utilises a TASMU Smart Service. They subscribe to and are authenticated by the TASMU Ecosystem. In some contexts they may be referred to as consumers.

[TASMU Ecosystem]

This is the Smart Qatar (TASMU) platform and any TASMU Smart Service that is either connected to this Central Platform or is branded as TASMU compliant. Refer to (A) in the TASMU Conceptual Diagram.

[TASMU Security Policy]

TASMU Security Policy, 2020, TASMU

[TASMU Smart Nation Regulator]

The entity in the State of Qatar who regulates the TASMU Ecosystem. It is responsible for drafting, promoting, governing, updating, monitoring compliance with, and enforcing this policy.

[TASMU Smart Service]

A TASMU Smart Service is a national service, leveraging one or multiple technologies, to resolve an identified challenge or enable a desired outcome and that operates in the TASMU Ecosystem. Collectively, they focus on detailing and contextualizing services relevant for the State of Qatar.

[TASMU Service Operator]

This is the owner and operator of the TASMU System, who has overall responsibility for its secure, compliant operation.

[TASMU System]

This is owned by the Service Operator and refers to any of the following elements from the TASMU Conceptual Diagram:

- (C) Any TASMU Smart Service
- (D) Any networking between platforms and (C)
- (E) Sector data analytics platforms
- (F) Central data analytics platform
- (G) Any networking between platforms and devices (H)
- (H) Any smart devices
- (I) The TASMU Control Centre
- (K) Security Management of the TASMU Ecosystem
- (L) Operations Management of the TASMU Ecosystem

[Terms of Service]

This sets out the contractual terms for a TASMU Smart Service and acts as the legal agreement between the TASMU Service Operator and a Subscriber. They incorporate items such as terms of use, costs/charges, licenses, termination, security and privacy provisions, etc.

1. Introduction

1.1 TASMU

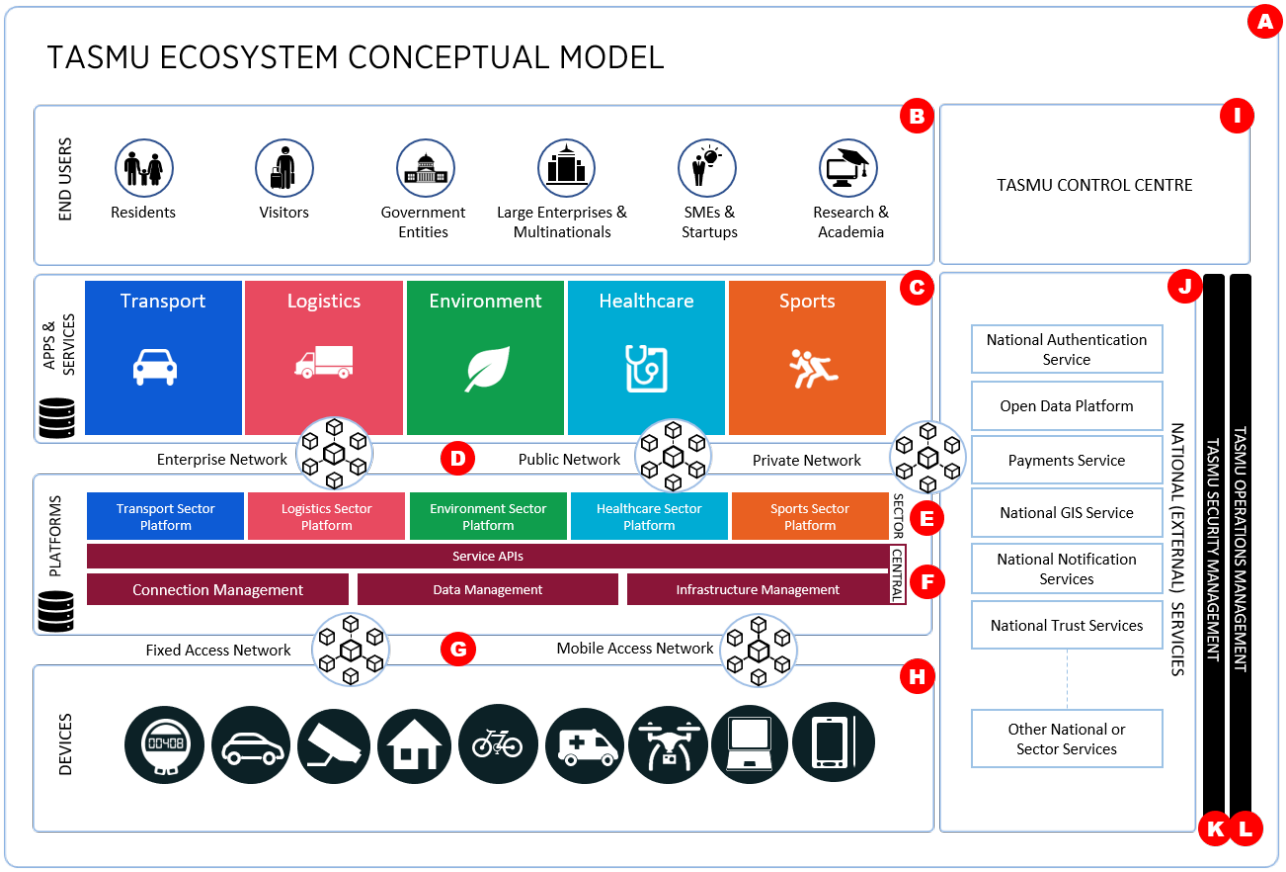
The Qatar National Vision 2030 aims to “transform Qatar into an advanced society capable of achieving sustainable development.” TASMU, or the Smart Qatar program, is a digital response to the goals that have been set out in the National

Vision 2030. It is about harnessing technology and innovation to improve quality of life and help drive economic diversification.

TASMU aims to leverage innovative applications of technologies to provide targeted services for residents, businesses and government across priority sectors. The foundation of this whole-of-nation effort relies on the ability to collect and manage vast amounts of data, share and open it up for spawning broad-based innovation and entrepreneurship within a set of defined rules and regulations. This is then processed and analysed by different actors for the build-up of innovative services and applications. As such, governance of TASMU on a national level has been designed to harmonize efforts across the different actors and drive Smart Qatar development with a key focus on ensuring efficiency and building resilience and interoperability.

TASMU Smart Services are services designed to solve evolving challenges targeted constituents (people, businesses, or government) face, leveraging technology and innovation. TASMU Smart Services cut across industry sectors focusing on human, social, economic, and environmental development. They can be focused on providing convenience or entertainment, or could address critical needs such as national safety and security. As such, the type of information they leverage can range from publicly open to sensitive or private information.

The policy covers the TASMU Ecosystem and interactions with it. The diagram below shows the TASMU Ecosystem in the context of this policy.



Only the following elements are within the scope of this policy:

- A: is the overall ecosystem
- B: is the end-user ecosystem
- C: is the TASMU Smart Services and services ecosystem
- D: are the network connections from the Central Platform, over enterprise, public and private networks
- E: are the sector data analytics platforms ('Sector Platforms')
- F: is the central TASMU data analytics platform ('Central Platform')
- G: is the Internet of Things (IOT) access network, either over fixed of wireless networks
- H: is the IOT devices ecosystem
- J: is the ecosystem of national services/platform that connects to the TASMU Central Platform and (C) above

1.2 Electronic Commerce & Transaction Policy

A wide range of policy areas affects e-commerce and e-commerce developments, and they must all be considered to support further innovations in the e-commerce marketplace. To ensure a full understanding of applicable controls, this policy should be read in conjunction with the TASMU Experience Policy.

The objective of this policy is to provide a consistent approach to electronic commerce and electronic transactions, within the TASMU Ecosystem especially where they are digitally signed or involve payment transactions. The aim is to ensure that all transactions within the TASMU Ecosystem can be used and accepted with a high level of confidence, easing their adoption for both commerce and legal requirements.

Electronic transactions within the TASMU Ecosystem require legal certainty to increase trust for Subscribers in TASMU Smart Services. This policy provides a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of smart services, electronic business and electronic commerce in the TASMU Ecosystem.

This TASMU policy is regulated by the TASMU Smart Nation Regulator.

1.3 Compliance

All TASMU Service Operators SHALL:

1. Comply with this policy where they operate a TASMU System or provide a TASMU Smart Service to a Subscriber, prior to operating in the TASMU Ecosystem and on a regular basis as directed by the TASMU Smart Nation Regulator.
2. Ensure that this policy is applied to all aspects of the TASMU System, whether that is maintained or operated by a third party, prior to operating in the TASMU Ecosystem.
3. Ensure this policy is considered in conjunction with the specific TASMU Smart Service sector policy issued by the TASMU Smart Nation Regulator or the sector regulator, which will cover specific requirements of the TASMU Smart Service.
4. Allow for an independent audit to check compliance, as and when necessary, or as directed by the TASMU Smart Nation Regulator.

2. Electronic Commerce

2.1 Service Operator Identification & Authenticity

1. The TASMU Service Operator SHALL be easily accessible and provide all Subscribers:
    a. their official name
    b. their contact information including email address
    c. their Commercial Register (CR) details
    d. any applicable licenses required for the TASMU Smart Service operation
    e. any code of conduct required for the TASMU Smart Service operation
2. If the TASMU Smart Service is a regulated service, the TASMU Service Operator SHALL provide all Subscribers:
    a. the details of professional entity or institution with which the TASMU Service Operator is registered
    b. the applicable professional title and the country where that title has been granted
    c. the professional rules or other rules applicable to the TASMU Service Operator in the country of authorisation or license, and the ways to access them
3. The TASMU Service Operator SHALL ensure that information directly related to the TASMU Smart Service is accurate and updated on a regular basis in line with any changes to the TASMU Smart Service. This includes information related to service availability, pricing, promotions, additional costs or fees.

4. The TASMU Service Operator SHALL ensure transparency and non-discrimination if they publish ratings or reviews by Subscribers.

5. Any promotions, discounts or competitions related to a TASMU Smart Service SHALL:

    a. be clearly and accurately identified, including whether it is a promotion, discount or other incentive
    b. ensure that any conditions to qualify for the incentive are not misleading or deceptive and presented clearly, unambiguously and are easily accessible.
    c. clearly define the start and end dates of the promotion, discount or competition

2.2 Service Operator E-Commerce Obligations

The TASMU Service Operator SHALL ensure:

1. If they are notified by the owner of any copyright protected content/work of a potential copyright infringement, the incident is investigated, and if the claim is valid the infringement is rectified in a timely manner.

2. Their contractual Terms of Service and their obligations for supporting Subscribers meet the requirements specified in the TASMU Experience Policy.

3. They clearly specify to Subscribers their right to withdraw from the contract, clearly stating the procedure, conditions, time limit, and with transparent mention of imposed withdrawal fees.

4. Subscribers are informed and given the opportunity to acknowledge that they are under obligation of carrying out and finalizing payment upon placement of their order. Subscribers are given the opportunity to agree or disagree with the possibility of explicitly agreeing to any additional payments imposed.

5. After an e-commerce order is placed:

    a. they confirm the contract as soon as possible, and no later than when goods are delivered, a service starts or digital content is downloaded
    b. provide a copy of the contract either by physical means (e.g. paper-based contract), or through electronic means (e.g. by email, text message, downloadable electronic document, etc.) which the Subscriber can save for future reference
    c. deliver the goods within thirty (30) days, unless agreed otherwise with the Subscriber

6. Personal Data is processed inline with §Personal Data Controls specified in the TASMU Security Policy, and Terms of Service incorporate all required obligations related to Personal Data.

2.3 Monetisation of Services

1. The TASMU Service Operator SHOULD ensure that their services are fairly monetised, and electronic payments are utilised, meeting the Contractual Terms of Service requirements specified in the TASMU Experience Policy.

2. The TASMU Service Operator SHALL ensure all prices are clear, unambiguous and do not contain hidden fees.

3. Where APIs are monetised the TASMU Service Operator SHALL meet the Availability and Reliability requirements specified in the TASMU Experience Policy.

4. Monetised APIs MAY be related to Data, Transaction, Application Integration, User Interface, Application Components, or be Utility and/or Helper APIs. These APIs SHOULD:

    a. have a clear financial model e.g. revenue sharing, indirect monetisation, usage based payment, etc.
    b. be packaged as a collection of related RESTful APIs as an API product
    c. follow rules to define which API calls qualify as monetised transactions and enforce monetisation limits on API proxies
    d. be PCI DSS compliant, specify terms and conditions, and support the use of Qatari Riyals (QAR)
    e. maintain traffic analytics to determine usage, allow continuous improvement and manage any abuse

f. implement the error handling and security controls specified in Application Interface Security and Portability requirements specified in TASMU Security Policy
g. be more useful over time by iterating based on API usage trends, user feedback, and other data
h. be scalable and elastic with minimal effort
i. comply with data governance, data ownership, data rights, data usage and data sharing as outlined in the TASMU Data Policy

2.4 Payments

The TASMU Service Operator SHALL ensure:

1. Subscribers can exercise an informed choice about available payment technologies by:

   a. clearly showing all available payment methods
   b. including details of any additional fees associated with using them, including, whereever feasible, foreign exchange costs
   c. providing guidance on using them

2. All payments related to the TASMU Smart Service are denominated in Qatari Riyals (QAR).

3. All electronic payments use encrypted channels, adhering to the requirements of the TASMU Security Policy.

4. All debit or credit card payments are compliant to the requirements of PCI DSS and the requirements on their acquiring banks.

5. Fraud detection and prevention in their payment channels is active 24 hours a day, seven days a week, 365 days a year (24/7/365) and updated in line with industry best practice, such as:

   a. monitoring transactions to identify inconsistencies e.g. inconsistent billing/shipping information, inconsistent physical location of customers, IP addresses from high risk hotspots
   b. checking against the Subscriber's purchase history for anomalies in purchasing behaviour
   c. checking the velocity and volume of transactions from the same Subscriber
   d. maintaining (and utilising) a grey list of chargebacks and disputes by delivery address
   e. using smart (AI/machine learning) risk based fraud rules, that are aligned to the TASMU Service Operator's business area, and provide behavioural tracking

6. Where possible, they use tokenization to replace sensitive cardholder data with a unique non-sensitive value.

7. They use additional protection for any "card-not-present" (CNP) transactions such as Address Verification Service (AVS), CVC2 Verification Service, 3DSecure v2.0 (3DS2), as best determined by their risk appetite.

8. If they utilise payment methods such as digital wallets, prepaid instruments, online banking e-payments or mobile payment systems, the Qatar Central Bank regulations are adhered to.

9. Subscribers have an effective method for initiating payment disputes e.g. for unauthorized payments, payment cancellations, unsuccessful transfers, etc.

3. Electronic Transactions

Within the TASMU Ecosystem TASMU Service Operators SHOULD use Electronic Transactions (with digital signatures, if required) instead of relying on paper based documentation and physical signatures. Apart from ease for the Subscriber, they are quicker and more efficient with better traceability of obligations and acceptance.

Electronic Transactions, requiring a high level of assurance and non-repudiation, SHALL meet the requirements specified in this section. They are subject to the provisions stated in the Electronic Commerce and Transactions Law.

3.1 Digital Signatures

1. Digital Signatures in the TASMU Ecosystem SHALL meet the following requirements:

    a. be uniquely linked to the Subscriber
    b. be capable of identifying the Subscriber
    c. are created using Signature Creation Information that the Signatory can, with a high level of confidence, use under their sole control
    d. linked to the data signed in such a way that any subsequent change in the data is detectable

2. Digital Signatures in the TASMU Ecosystem SHALL adopt the following standards, specified in the Electronic Signature Formats standard:

    a. be of a format compatible with CAdES [ETSI EN 319 122] or XAdES [ETSI EN 319 132] or PAdES [ETSI EN 319 142]
    b. be created and validated in applications meeting the policy and security requirements of [ETSI TS 119 101] or equivalent

3. Digital Signatures MAY use any profile type (basic, timestamped, with revocation information, with signature policies etc.) as determined by the risk and assurance needs of the transaction, and as agreed between the community of users.

4. Signature Creation Information SHALL be stored commensurate to the assurance requirements of the transaction. Options MAY include:

    a. encrypted storage files (low assurance)
    b. operating system keystores (low assurance)
    c. cryptographic tokens and smart cards (medium assurance)
    d. Trusted Platform Modules (TPMs) (medium assurance)
    e. Hardware Security Modules (HSMs) (high assurance)

5. Where Digital Signatures are used on mobile devices holding Signature Creation Information, or used for cloud based signing where the Signature Creation Information is held in the cloud, or where signature validation takes place in the cloud, the standards provided in [ETSI SR 019 020] SHOULD be used.

6. Certificate Service Providers (CSPs) enabling Digital Signatures SHALL meet the policy and security requirements of [ETSI EN 319 411] or equivalent.