ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3059 (12/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Future networks

Trust registry for devices – Requirements, architectural framework

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	**Y.3000-Y.3499**
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3059

Trust registry for devices – Requirements, architectural framework

Summary

The world is witnessing a massive proliferation of connected devices and services that affect every walk of life. The security threats from this vast, distributed and often unregulated emerging ecosystem of providers of devices and applications are also clear to the world. Recommendation ITU-T Y.3059 defines the requirements that are to be fulfilled by a trust registry that, when supported by the various stakeholders, is likely to create an environment for the sustainable and orderly proliferation of secure devices.

Requirements, an architectural framework for a hierarchy of registries, functional architecture and flows for the registration, interrogation and notification throughout the lifecycle of devices is proposed, with the objective that the trustworthiness of a device can be established at any point in time.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3059	2023-12-14	13	11.1002/1000/15734

Keywords

Authentication, geographical registry, primary registry, registered device identity, registry hierarchy, registry identity, sectoral registry, trust registry, trusted device.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3059

Trust registry for devices – Requirements, architectural framework

1 Scope

This Recommendation includes:

– Overview of trust registry and hierarchy;

– Requirements for registration, interrogation and notification pertaining to the trustworthiness of the connected devices throughout the lifecycle;

– Requirements for root(s) of trust (RoT) and reference points to enable the mechanisms and functions of the trust registry;

– An architectural framework for the hierarchical set-up of trust registries belonging to various domains, sectors and/or geographical areas; and

– Functional architecture and flows for the registration, interrogation and notification of the trustworthiness of devices.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3410] Recommendation ITU-T M.3410 (2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[ITU-T Y.3056] Recommendation ITU-T Y.3056 (2021), *Framework for bootstrapping of devices and applications for open access to trusted services in distributed ecosystems*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 trust domain [ITU-T M.3410]: A set of information and associated resources consisting of users, networks, data repositories, and applications that manipulate the data in those data repositories. Different trust domains may share the same physical components. Also, a single trust domain may employ various levels of trust, depending on what the users need to know and the sensitivity of the information and associated resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 primary registry: The lowest level hierarchy among trust registries, representing a basic useful common context, with several other domain peers.

3.2.2 sectoral registry: A registry that contains and serves several primary registries and is parented to a single geographical registry, with several other sectoral peers.

3.2.3 geographical registry: A registry that contains and serves several sectoral registries and may have other geographical registry peers.

3.2.4 registry identity (RegID): An identifier assigned to a trust registry.

3.2.5 registered device identity (RegDevID): A unique identifier issued to a registered device by a registry.

3.2.6 virtual registered device identity: A temporary identifier, linked with the RegDevID of a registered device, which can be generated as a temporary identifier for a specified time period / single transaction in order to protect the RegDevID.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CoAP	Constrained Application Protocol
EIR	Equipment Identity Register
GSM	Global System for Mobile communications
GSMA	GSM Association
GUID	Globally Unique Identifier
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
RegDevID	Registered Device Identity
RegID	Registry Identity
RoT	Root(s) of Trust
TAC	Type Allocation Code
UE	User Equipment

5 Conventions

In this Recommendation, requirements are classified as follows:

- The keywords "**is required to**" or "**are required to**" indicate requirement(s), which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.
- The keywords "**is recommended**" indicate a requirement, which is recommended but which is not absolutely required. Thus, such requirements need not be present to claim conformance.
- The keywords "**optionally**" or "**may**" indicates an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option; it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Trust registry overview and background

6.1 Trust registry overview

The trust registry is a means to mitigate the security threats from the proliferation of largely unregulated connected devices which are becoming a part of our personal and professional lives. The trust registry requirements create an environment of trust for various stakeholders that contribute to the ecosystem. The overview, architectural framework, functional architecture and flows related to the trust registry are provided to support the use cases for the registration, interrogation and notification related to the connected devices, with the objective that the trustworthiness of a device can be established at any point in time in its lifecycle.

The Recommendation provides that the registration of devices to the trust registry is based on roots of trust that host identities, keys, certificates and protocols to ensure that the principles of security by design can be implemented. The constraints related to low cost IoT devices are kept in mind to ensure inclusivity.

The trust registry security framework is based on [ITU-T Y.3056], which specifies the use of security tokens for verifying the identity of the connected device and ensuring end to end communications security. The trust registry permits the use of existing device identifiers to ensure ease of use for all the stakeholders.

The trust registry issues an identity to each registered device that provides a meaningful disclosure of the device's type, its network connectivity capability and other similar attributes. In some cases, the issued identity subsumes the network provided identity making it easy to recognize and transact with the device.

The need for having a hierarchy of registrars may require that several types of trust registries are recognized in the trust registry model. At least three types of registrars are apparently needed – the geographical registry, sectoral registry and primary registry.

It may be noted that each trust hierarchy layer such as primary, sectoral and geographical area layer may have multiple trust registries and each of these may require the existence of trust domains [ITU-T M.3410] that may employ various levels of trust mechanisms, depending on the use-case requirements and user's need for sensitivity, privacy and security of the information and associated resources. Different trust domains may share the same physical components as far as the user devices and applications are concerned.

An overview of the trust registry hierarchy is provided in Figure 1. This is an illustrative diagram to demonstrate the concept of the trust hierarchy. There can be any number of different hierarchies, and within each hierarchy, any number of trust registry entities. There could be models within which the registries may interact bilaterally.

Using the diagram below, the following important matters related to trust registry hierarchy may be summarized.

– The illustration in Figure 1 shows a three-level hierarchy model in which there is a geographical area trust registry layer at the apex, an intermediate sectoral trust registry layer and a lowest layer named the primary trust registry.
– Each trust registry layer may have one or more trust registries.
– The trusted devices are registered at the primary registry layer using roots of trust per [ITU-T Y.3056].
– The database of each registry maintains the list of registered trusted devices along with their current state in terms of their trust status.
– The trust status of a trusted device or application can be either trusted, unverified or unreliable.

– The trust registries across layers maintain and notify the status of trust of the trusted device or application across its lifecycle.

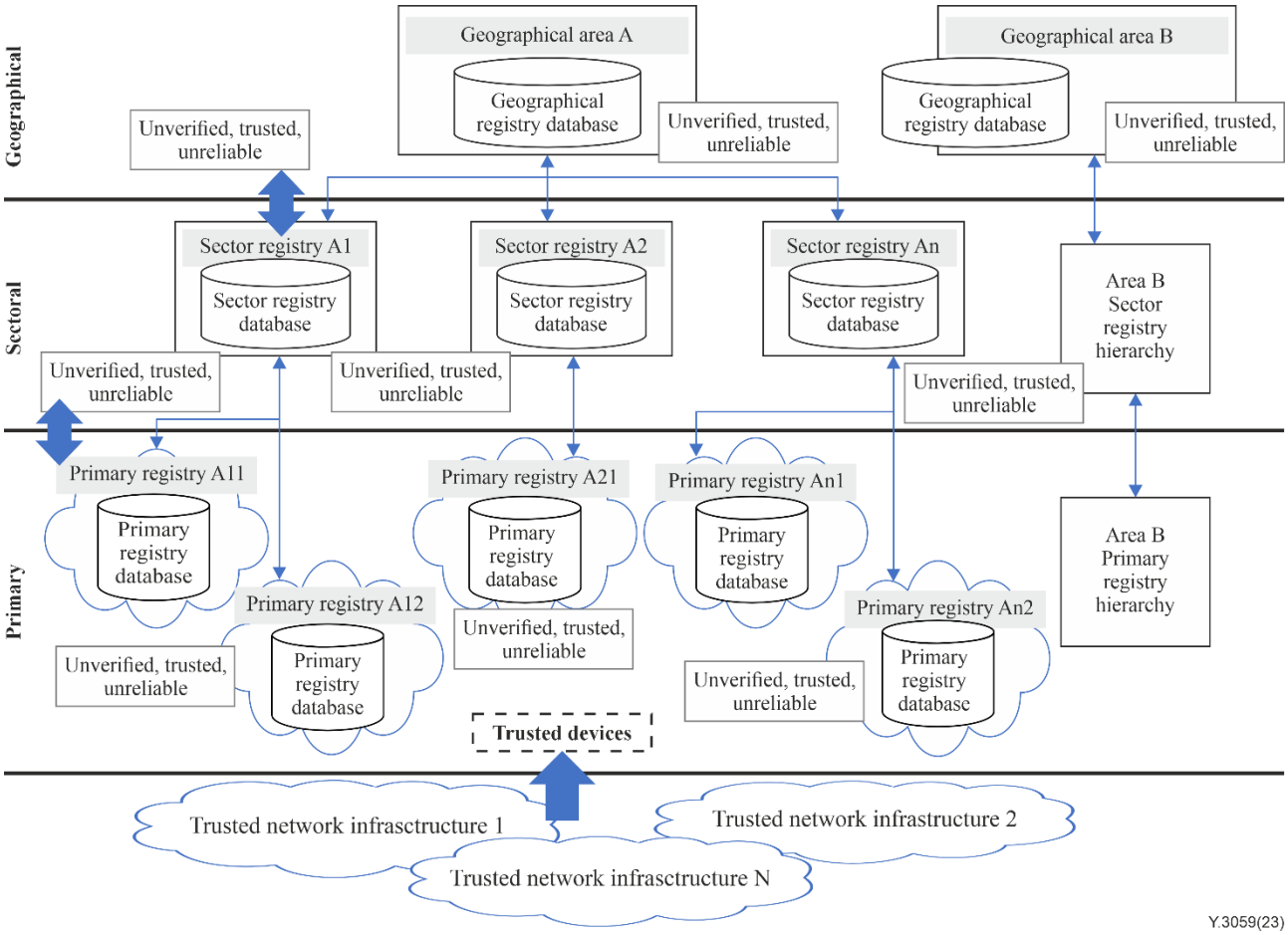

Figure 1 – Trust registry hierarchy

6.2 Background

The proliferation of connected devices serving a wide variety of use cases across different industry verticals presents both challenges and opportunities for uniform and global identification and verification.

Some of the key challenges for uniform and global identification and verification are as follows:

- **Wide variety of computing and communication technologies, interfaces and protocols**: Connected and other devices vary hugely in complexity and capability as it relates to computing and communication, making it hard to use either the processor or communications interface as a uniform and global identification and verification mechanism.
- **Lack of standardization**: There are currently many accepted standards for device identification and verification. The fact that there are many options – for many use cases – reflects the flexibility of managing device identity, but for those wanting a single, universal solution, this variety of standards leads to fragmentation and inconsistency in device management.
- **Heterogeneity of devices**: Connected devices come in various shapes, sizes and configurations, making it difficult to develop a one-size-fits-all identification and verification solution.
- **Security risks**: The connected nature of connected devices presents significant security risks, and identifying and verifying devices can be an essential part of mitigating those risks.

- **Privacy concerns**: The identification and verification of connected devices can raise privacy concerns, particularly when it comes to personal data collection and sharing.

Although a uniform process for the global identification and verification of connected devices is a significant challenge, having such a system presents significant benefits and opportunities:

- **Enhanced security**: A uniform global device identification and verification system can help mitigate security risks and protect against cyberattacks.
- **Improved device management**: A uniform and global identification and verification system can streamline device management and enable more efficient and effective device monitoring and maintenance.
- **Better interoperability**: A standard identification and verification system can significantly improve interoperability between different devices and systems, making it easier to identify the devices and their capabilities, and integrate them into various applications across use cases from different industries.
- **Improved user experience**: A streamlined global identification and verification process can dramatically improve the user experience for both individuals and organizations, enabling them to quickly and easily connect and manage devices.

In conclusion, while the challenges of uniform and global identification and verification of connected devices are significant, the opportunities for improved device management, enhanced security, better interoperability and improved user experience make it important to be pursued. A collaborative effort between stakeholders, standardized across industries and regions, is necessary to develop and implement a uniform and global identification and verification system that meets the diverse needs of connected device ecosystems.

6.3 Trust registry versus agency issuing globally unique identifiers

This introductory text is meant to clarify the different purposes served by a registry and an agency issuing globally unique identifiers (GUIDs). Although both are involved in the management of unique identifiers, and hence may look similar, they have different roles and responsibilities. Some key differences between the two are the following:

a) **Definition**: A registry is a database or system that stores and manages information about specific resources, such as domain names, IP addresses or device identifiers. In contrast, a GUID issuing agency is responsible for assigning and distributing unique identifiers to entities that require them, such as organizations or individuals, e.g., a type allocation code (TAC) issued by GSMA for user equipment (UE) provides information in respect of the manufacturer and model of the item of UE, but will not provide information as to whether particular UE is trusted or who is the owner/ custodian of it.

b) **Function**: A registry serves as a central repository of information for a particular resource, providing authoritative information about its ownership and trust status. A GUID issuing agency, on the other hand, creates and assigns unique identifiers to entities that need them, ensuring that each identifier is globally unique and unambiguous.

c) **Scope**: A registry is typically focused on a specific resource, such as domain names, IP addresses or devices. In contrast, a GUID issuing agency may be responsible for issuing unique identifiers across a broad range of resources, including devices, software applications and services.

d) **Authority**: A registry is typically operated by a neutral third party, such as a domain name registrar or a regional Internet registry, and serves as an authoritative source of information about a specific resource. In contrast, a GUID issuing agency is typically designated by a governing body or standards organization, such as the International Organization for Standardization (ISO), and is responsible for ensuring that unique identifiers are assigned in accordance with established guidelines and procedures.

e) **Governance**: A registry is typically subject to specific policies and procedures that govern how the resource is managed and allocated, including rules for registering, transferring and revoking ownership of a specific resource. A GUID issuing agency, on the other hand, is responsible for establishing procedures for issuing unique identifiers, including ensuring that each identifier is globally unique and unambiguous.

In summary, a registry and an agency issuing GUIDs play very different roles in the management of unique identifiers. A registry serves as a central repository of information about a specific resource, while a GUID issuing agency creates and assigns unique identifiers to entities that require them. Both are essential components of the digital ecosystem, and their effective management is critical to ensuring the standardization, interoperability and sustainability of the connected devices ecosystems.

7 Requirements

The trust registry imposes requirements for the registration and lifecycle management of trusted devices, manufacturers and owners/custodians; vulnerability disclosure, recording and controlled dissemination; interrogation of the registry and the registered trusted devices; notifications from the registry; and exchange of device information between registries. Accordingly, the requirements for the trust registry, root(s) of trust (RoT), devices and reference points are listed below.

i) The trust registry is required to:

   a) Provide appropriate mechanisms for securing access to the registry for the administrators and users of the trust registry;

   b) Ensure that appropriate mechanisms are deployed for securing access to the trusted devices based on the use of suitable encryption; and

   c) Ensure recording, logging and/or auditing the transactions undertaken by the trust registry.

ii) Root(s) of trust is required to:

   a) Provide an inviolable foundation over which the trust registry security and trust flows and mechanisms can be built; and

   b) Have a highly reliable tamperproof hardware, firmware and software that can be inherently trusted.

iii) The devices registered to the trust registry are required to have RoT.

iv) The reference point is required to have following capabilities in order to enable:

   a) A device to request a registration (register) to the primary trust registry;

   b) The trust registry to communicate the RegID (acknowledge) to the trusted device and confirm the acceptance of the RegID by the device (det);

   c) The transfer of security parameters from the device to the trust registry (report);

   d) The exchange of trusted/unverified/unreliable lists between the trust registries based on vulnerability reports received at the primary or other registry based on real-time transactions occurring in the lifecycle of trusted devices, to create an updated and synchronized trust status of the trusted devices;

   e) The ability to publish/subscribe a variety of use-case-based trust status information related to the trusted devices, both in response to interrogation by enquirers, and a proactive notification by trust registries; and

   f) The real-time exchange and update of trust status of the trusted devices between trust registries.

8 Architectural framework for trust registry hierarchy

The model of the trust registry framework is shown in Figure 2.

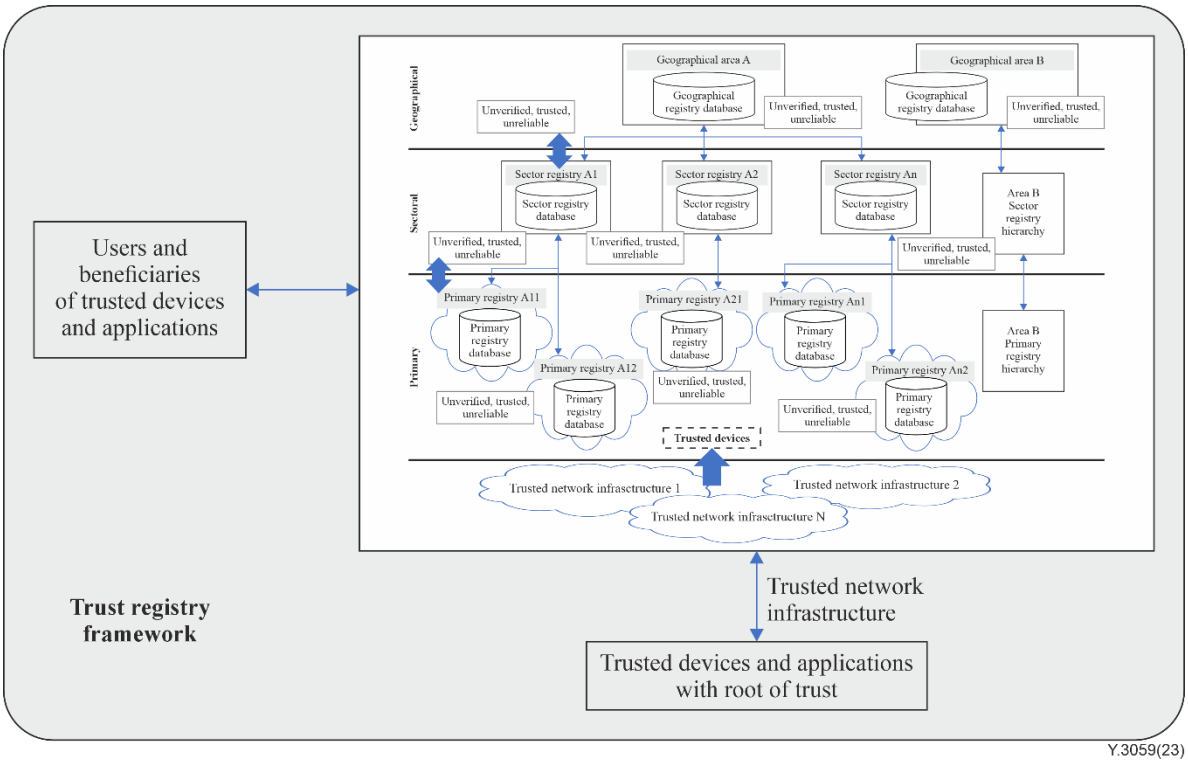

Figure 2 – Model for trust registry framework

The trust registry hierarchy entities interact with the users and beneficiaries to notify the trust status of the trusted devices enabled by trusted network infrastructure.

The primary trust registries register trusted devices that are verified by the trusted network infrastructure. The layers of the trust registry provide interfaces that can be interrogated by the users and beneficiaries to securely verify the trust status of trusted devices using parameters such as make, model, capabilities, trust attributes and ownership.

NOTE – The approach in this Recommendation is generic in nature, independent of the operator and network technology.

8.1 Functional architecture

The trust registry functions have been analysed to identify generic functionality which is independent of implementation technology. This analysis results in a description of trust registry functionality in an abstract way in terms of a few components of a functional architecture. These components are defined by the function they perform in processing information and in terms of the relationships they have with other architectural components. In general, the functions described here are defined and characterized by the information process between their inputs and outputs. They act on information provided at one or more inputs and relay processed information at one or more outputs.

The trust registry functional architecture is provided in Figure 3.

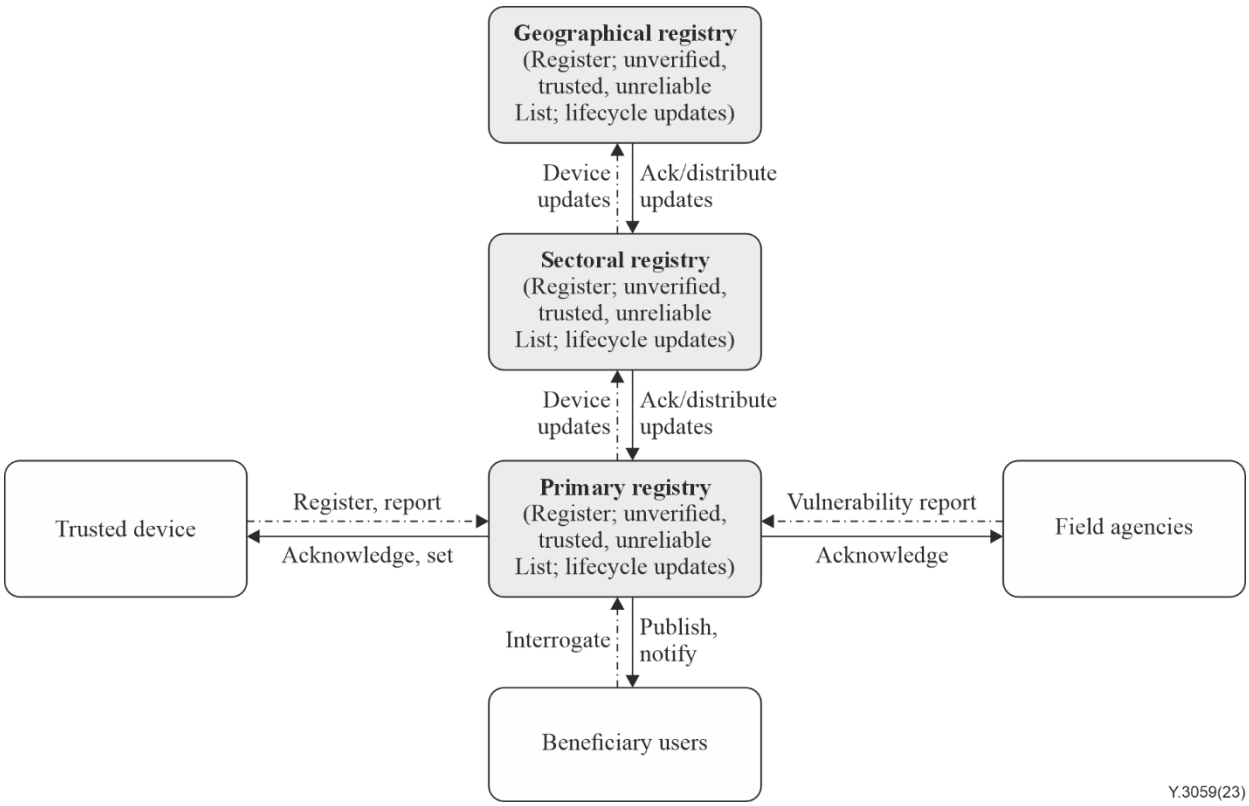

Figure 3 – trust registry functional architecture

9 Mechanisms and flows

The mechanisms and flows provided here set out the principles and practices for creating and using the trust registry.

NOTE – Clauses 9.1 and 9.2 describe the process of the registration of a trusted device to a trust registry, the security of the information flows is required to be per [ITU-T Y.3056].

9.1 Set-up and securing access to the trust registry

The set-up and securing of the access to the trust registry requires the following capabilities:

i) A mechanism for providing a unique name/identity to the trust registry. The naming may have a number of characters that allow sufficient number of expected unique names e.g., if it is expected that there will be a total of 100 registries including the geographical, sectoral and primary registries, a numbering "xxx" may be considered, where "x" can be a character from A to Z and/ or a number from 0 to 9 or a combination of both;

NOTE – If a geographical area already has a popularly used unique digital identity issued by an international naming/numbering agency such as ICANN or GSMA, then, for sake of simplicity, such naming/numbering may be used as the geographical area registry identifier.

ii) A mechanism for assignment of a trust registry type – primary, sectoral or geographical;

iii) A mechanism for securing access to the registry and the personally identifiable information of the owners/custodians stored in the registry by the administrators and users of the trust registry;

iv) A mechanism for securing access to the registry for querying the trusted devices that are registered at the trust registry;

v) A mechanism for securing the interactions between trust registries, e.g., use of [b-IETF RFC 8996] for secure server interactions; and

vi) A set of published acceptable roots of trust, keys/certificates and protocols for securing the registration and access to trusted devices.

NOTE – Clause 9.1 (iii) refers to the securing of access to information available in a trust registry which may be related to the trusted devices. Clause 9.1 (iv) refers to securing of access to the devices that are registered in the trust registry.

9.2 Registration of a trusted device and the device owner/ custodian

The capabilities required for the registration of a trusted device and the device owner/ custodian to a trust registry are listed below.

i) The trust registry should be capable of:

a) Authenticating the trusted device using cryptographic processes involving the root of trust, keys/certificates, and protocols that are stored in the device's secure element;

b) Adding its geographically unique registry identity (RegID) (prefix or suffix) to the connected device's inherent unique identifier (viz. IMEI, MAC, IPv6 or other such unique digital identifier) to generate a geographically unique registered device identifier RegDevID and assign it to the trusted device;

c) Communicating the RegDevID to the trusted device;

d) Storing and verifying the information related to the identity of the owner/custodian of the trusted device;

e) Storing the information related to the trusted device such as make, model, root of trust, unique device identity, firmware/software version, communication capabilities, power capabilities, device status (trusted list / unverified list/ unreliable list), protocols supported e.g., MQTT, HTTP and CoAP;

f) Providing a facility for the issuance of a virtual RegDevID; and

g) Providing support for single or bulk operations related to the registration of trusted devices and, wherever required, the device owners/custodians.

ii) The trusted device should be capable of:

a) Registering to the trust registry by using its geographically unique identity that is stored in its tamper resistant secure element;

b) Accepting and securely storing the RegDevID;

c) Securely using the RegDevID for its identification and authentication by the trust registry;

d) Providing information such as make, model, root of trust, unique device identity, firmware/software version, communication capabilities, power capabilities, protocols supported e.g., MQTT, HTTP and CoAP.

NOTE – A device is always registered to a trust registry through the trusted network infrastructure. Once registered, a registry can interrogate a registered device per clause 9.3.

9.3 Trust registry interrogation

The capabilities required for the interrogation of a trusted device to a trust registry are as follows:

i) The trust registry should be capable of communicating:

a) A set of procedures for enquirers to register and authenticate themselves to query the Registry;

b) A detailed practice statement so that the various beneficiaries, including, but not limited to, manufacturers, users, owners/custodians and registries can know the process and facilities available from the trust registry;

c) A set of procedures for devices to update the trust registry with its security parameters on a periodical basis, by using its geographically unique identity and cryptographic processes involving the root of trust, keys/certificates and protocols that are stored in the device's secure element;

ii) The trust registry should be capable of:

a) Accepting and securely storing the data sent by the trusted devices against the RegID of the device by using a date/time stamp against each such update such as to maintain a detailed view of the security parameters of the trusted device throughout its lifecycle;

b) Storing the complete set of information related to the vulnerabilities of the trusted device by using a date/time stamp against each such information update that is received from the device, the owner/custodian, other registries or other agencies authorized for such a purpose;

c) Handling single operations related to the interrogation of trusted devices, and the associated owners/ custodians; and

d) With appropriate security procedures for restricted access to trust repository administrators, handling bulk operations related to interrogation of trusted devices, and the associated owners/custodians, if required.

iii) The trust registry and the trusted device should be capable of providing the enquirer an immediate set of security challenges and provide access to information only when the challenge-response mechanism has successfully authorized the access to information; and

iv) The trusted device should be capable of providing, and the trust registry should be capable of storing, the initial information and all the changes related to the trusted device security parameters such as changes in the firmware and communication capabilities.

9.4 Trust registry notifications

The capabilities required for the facilities related to notifications offered by a trust registry are as follows.

i) The trust registry should be capable of communicating:

a) A set of procedures for enquirers and beneficiaries to register and authenticate themselves to obtain notifications from the trust registry;

b) A set of procedures for devices and registries to exchange updates regarding the trusted device security parameters and vulnerability information; and

c) Certain information regarding devices on a periodical basis, and certain other information on an event basis.

ii) The trust registry should be capable of providing a facility for single or bulk notification operations related to trusted devices, as required.

10 Security considerations

This Recommendation proposes the existence of multiple trust registries with a hierarchical structure based on clause 6, which may register connected devices that belong to both IP and non-IP network realms. The security of the information flows between the registry and the trusted devices is required to be per [ITU-T Y.3056]. Thus, the security and privacy considerations are based on clauses 7 and 8 of [b-ITU-T Y.2701]. Additional information can be found in [b-ITU-T Y Sup19].

In order to mitigate security threats and potential attacks, issues of confidentiality, integrity, authenticity, non-repudiation, availability and traceability need to be addressed, and appropriate security and privacy protection schemes should be considered for the trusted devices, applications and the interfaces between these and the network realms. Details are outside the scope of this Recommendation.

Bibliography

[b-ITU-T Q.5052] Recommendation ITU-T Q.5052 (2020), *Combating counterfeiting and stolen ICT devices Addressing mobile devices with a duplicate unique identifier*.

[b-ITU-T Q.5053] Recommendation ITU-T Q.5053 (2021), *Combating counterfeiting and stolen ICT devices Mobile device access list audit interface*.

[b-ITU-T Q Suppl.73] ITU-T Q-series Supplement 73 (2021), *Guidelines for permissive versus restrictive system implementations to address counterfeit, stolen and illegal mobile devices*.

[b-ITU-T Q Suppl.75] ITU-T Q-series Supplement 75 (2021), *Use cases on the combat of counterfeit ICT and stolen mobile devices*.

[b-ITU-T Q Suppl.76] ITU-T Q-series Supplement 76 (2023), *Common approaches and interfaces for data exchange between CEIR and EIR*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y Sup19] ITU-T Y.Sup19 (2012), *Supplement on the risk analysis service in next generation networks*.

[b-IETF RFC 8996] IETF RFC 8996 (2021), *Deprecating TLS 1.0 and TLS 1.1*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2024