Draft new Recommendation ITU-T Y.3059 (ex.Y.Trust-Registry)

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. This recommendation defines the requirements that is required to be fulfilled by a trust registry that, when supported by the various stakeholders, is likely to create an environment for 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.

Keywords

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

Table of Contents

Draft new Recommendation ITU-T Y.3059 (ex.Y.Trust-Registry)

Trust Registry for Devices: requirements, architectural framework

1 Scope

The 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 and reference points to enable the mechanisms and functions of the trust registry;
- An architectural framework for the hierarchical setup 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 (08/2008), *Guidelines and requirements for security management systems to support telecommunications management*.

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (03/2017), *Overview of trust provisioning in information and communication technology infrastructures and services*.

[ITU-T Y.3056] Recommendation ITU-T Y.3056 (02/2021), *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 terms 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**: A primary registry is the lowest level hierarchy amongst trust registries, representing a basic useful common context, with several other domain peers.

3.2.2 **sectoral registry**: A sectoral registry 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 geographical registry 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:

CCTV	Closed Circuit Television
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
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
RegID	Registry Identity
RegDevID	Registered Device Identity
RoT	Root(s) of Trust
TAC	Type Allocation Code (issued by GSMA)
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; and
- The keywords "**optionally**" or "**may**" indicate 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 the [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, which identity 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 recognise and transact with the device.

The need for having a hierarchy of registrars may require that several types of trust registries are recognised 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 below. 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 in which the registries may interact bilaterally.

Using the diagram below, the following important matters related to Trust Registry hierarchy may be summarised.

- The illustration in the 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 as per the [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 White (trusted), Grey (Unknown) and Black (rogue).
- The Trust Registries across layers maintain and notify the status of trust of the Trusted Device or Application across its lifecycle.

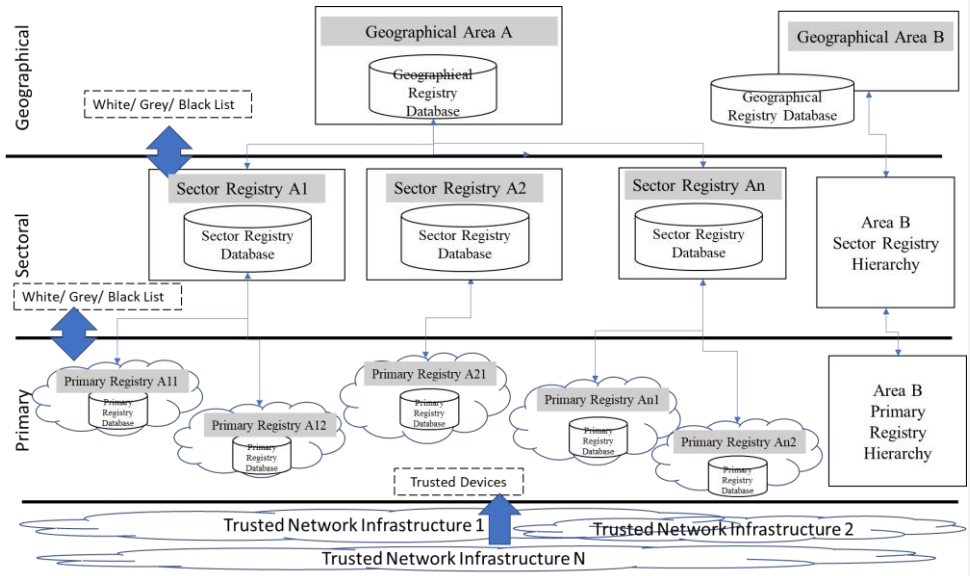


Figure 1: Trust Registry Hierarchy

6.2 Background

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

Some of the key challenges for uniform and global identification and verification are listed below:

- **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 is currently no universally accepted standard for device identification and verification, leading to fragmentation and inconsistency in device management.~~ *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 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, standardised 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 (GUID). Although both agencies are involved in the management of unique identifiers, and hence they may look similar, but they have different roles and responsibilities. Some key differences between the two are discussed below:

(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 UE, but will not provide information as to whether a particular UE is trusted or who is the owner/ custodian of the UE.

(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 standardisation, interoperability and sustainability of the connected devices ecosystems.

7 Requirements

The trust registry imposes requirements for 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, 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) The Root(s) of Trust (RoT) 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 a Root(s) of Trust (RoT).

(iv) The Reference Point (RP) 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 (Set);

(c) the transfer of security parameters from the Device to the Trust Registry (Report);

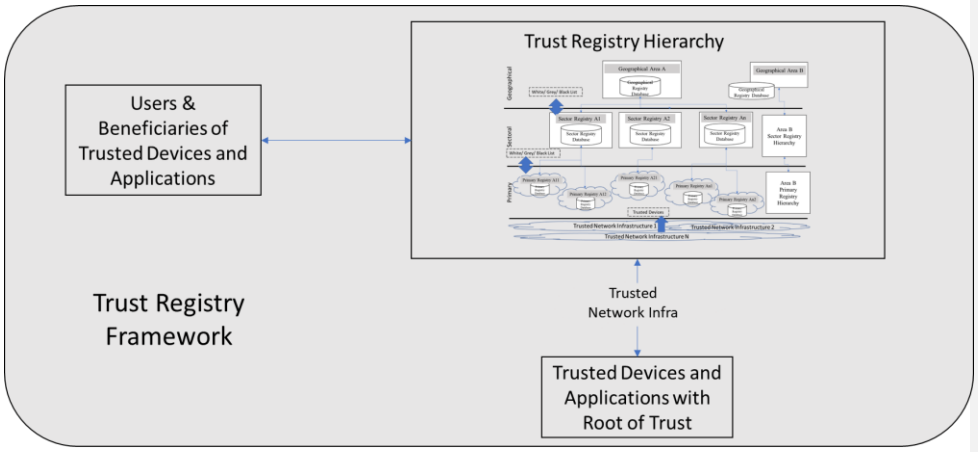
(d) the exchange of White/ Grey/ Black Lists between the Trust Registries based on vulnerability reports received at the Primary or other Registry based on real-time transactions occurring in the lifecycle of trusted devices, to create an updated and synchronised trust status of the trusted devices;

(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 provided in Figure 2 below:



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 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.

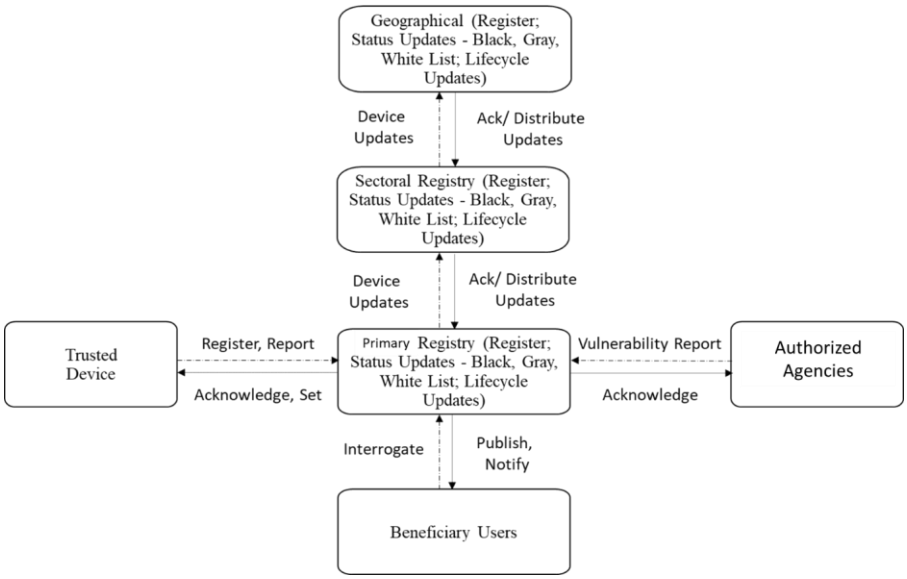
Figure 2: Model for Trust Registry Framework

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 below:



Commented [AV1]: Please replace "Field Agencies" with "Authorized Agencies" in this diagram

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 below describe the process of the registration of a trusted device to a trust registry, the security of the information flows is required to be as per [ITU-T Y.3056].

9.1 Setup and Securing access to the Trust Registry

The setup 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, GSMA, etc., 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 & 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 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: 9.1 (iii) refers to the securing of access to information available in a trust registry which may be related to the trusted devices. 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 (Blacklist/ Whitelist/ Grey List), protocols supported e.g., MQTT, HTTP, CoAP etc.;
   (f) providing a facility for the issuance of a virtual RegDevID; and
   (g) providing support for single or bulk operations related to 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, CoAP etc.

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

9.3 Trust Registry Interrogation

The capabilities required for the interrogation of a trusted device to a Trust Registry is listed below.

(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, registries, etc 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 authorised for such purpose;
   (c) handling single operations related to 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 authorised 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, communication capabilities etc.

9.4 Trust Registry Notifications

The capabilities required for the facilities related to notifications offered by a trust registry is listed below.

(i) The Trust Registry should be capable of communicating:
   (a) a set of procedures for enquirers and beneficiaries to register and authenticate themselves to get 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 having 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 as 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-Sup.19].

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 Y.2701] Recommendation ITU-T Y.2701 (04/2007), *Security requirements for NGN release 1*.

[b-ITU-T Y-Sup.19] ITU-T Y.2200-series Supplement 19 (06/2012), *Supplement on the risk analysis service in next generation networks*.