Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-wang-data-transmission-security-irii-03
Published: 13 September 2022
Intended Status: Standards Track
Expires: 17 March 2023
Authors: B. Wang, Ed. Hikvision
K. Lin, Ed. Hikvision
C. Wang, Ed. IIE, CAS
X. Wang, Ed. Hikvision

Data Transmission Security of Identity Resolution in Industrial Internet

Abstract

This draft provides an overview of the security of data transmission in the identity resolution system for the Industrial Internet. Identity resolution systems play a vital role in the Industrial Internet by providing secure sharing and intelligent association of heterogeneous information among different organizations. This draft focuses on the security services that identity resolution systems should provide for resolution data transmission.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 17 March 2023.

Copyright Notice

Table of Contents

1. Introduction

Identity resolution system is an important network infrastructure for the Industrial Internet. It provides codes, registration and resolution services for industrial equipment, machines, materials, parts and products to achieve interoperability, secure sharing and intelligent association of heterogeneous information, which is an important cornerstone for the rapid development of the Industrial Internet. Typical global identity resolution systems in existence include the Handle system [RFC3650] [RFC3651], the Object Identifier (OID) resolution system [OID], etc. In order to ensure the security of data transmission involved in the Industrial Internet identity resolution systems, the security technical requirements are

formulated to enhance the security of the entire Industrial Internet identity resolution system and reduce the security risk caused by data leakage. The security technical requirements can be applied to the planning, construction, operation and management of data transmission security of Industrial Internet identity resolution systems.

2. Scope

This draft specifies the security technical requirements for the transmission of Industrial Internet identity resolution data.

This draft applies to the planning, construction, operation and management of the Industrial Internet identity resolution data transmission security of the relevant parties.

3. Terms and Definitions

3.1. International Root Node

International root nodes are the top-level service node of the identity resolution system. They are not limited to specific countries or regions. Their main role consists of two aspects: (1) to provide public root-level identity services for the global scope; (2) and to provide services such as data synchronization and registration resolution for different levels of nodes in local country.

3.2. National Root Node

A national root node is the top-level node within a country or a region, which is connected to the international root node and secondary nodes, provides top-level identity resolution services for the whole country.

3.3. Secondary Node

A secondary node is a public node providing identity services for specific industries or multiple industries. Secondary node is responsible for allocating identity and providing identity registration, identity resolution and identity data services for industrial enterprises. Two types of secondary nodes exist, namely industry secondary nodes and comprehensive secondary nodes.

3.4. Enterprise Node

An enterprise node is an intra-enterprise identity service node which is able to provide identity registration, identity resolution service and identity data service for a specific enterprise. An enterprise node should be connected to a secondary node.

3.5. Recursive Node

A recursive node is the key entrance facility of the identity resolution system, whose responsibility is to cache the resolution data in the process of identity resolution, in order to reduce the amount of resolution data processing and improve the efficiency of resolution services.

3.6. Transmission Security

Protect the confidentiality, integrity, availability and timeliness of data transmitted over the network.

3.7. Privacy

Privacy refers to the authority that individuals have to control their information, including who collects and stores it and who discloses it.

3.8. Personal Data

Personal Data refers to the information that a natural person can be identified directly through the data, or indirectly through the data combined with other information.

4. Abbreviation

Abbreviation	Full Name
TLS	Transport Layer Security
IPSec	Internet Protocol Security
HTTPS	Hypertext Transfer Protocol Secure
OID	Object Identifier
DNS	Domain Name System
ENODE	Enterprise Node
IIP	Industrial Internet Platform
HandleID	Unique Identification of Equipment

Table 1: Abbreviation

5. Overview

The Industrial Internet identity resolution and management service system is mainly a system that supports the global traceability management of industrial IoT product data and dynamic sharing of data information in all aspects of the product life cycle by using the capabilities of the security identity management and resolution platform. Industrial Internet identity resolution data transmission refers to the data technology collection used in the Industrial Internet terminal to obtain information and transmit information,

and its transmission security involves the network security part of the basic security protection measures dimension, all inter-domain and intra-domain data transmission of the functional domain dimension of the Industrial Internet identity resolution and management service system, and the whole process of the system life cycle dimension.

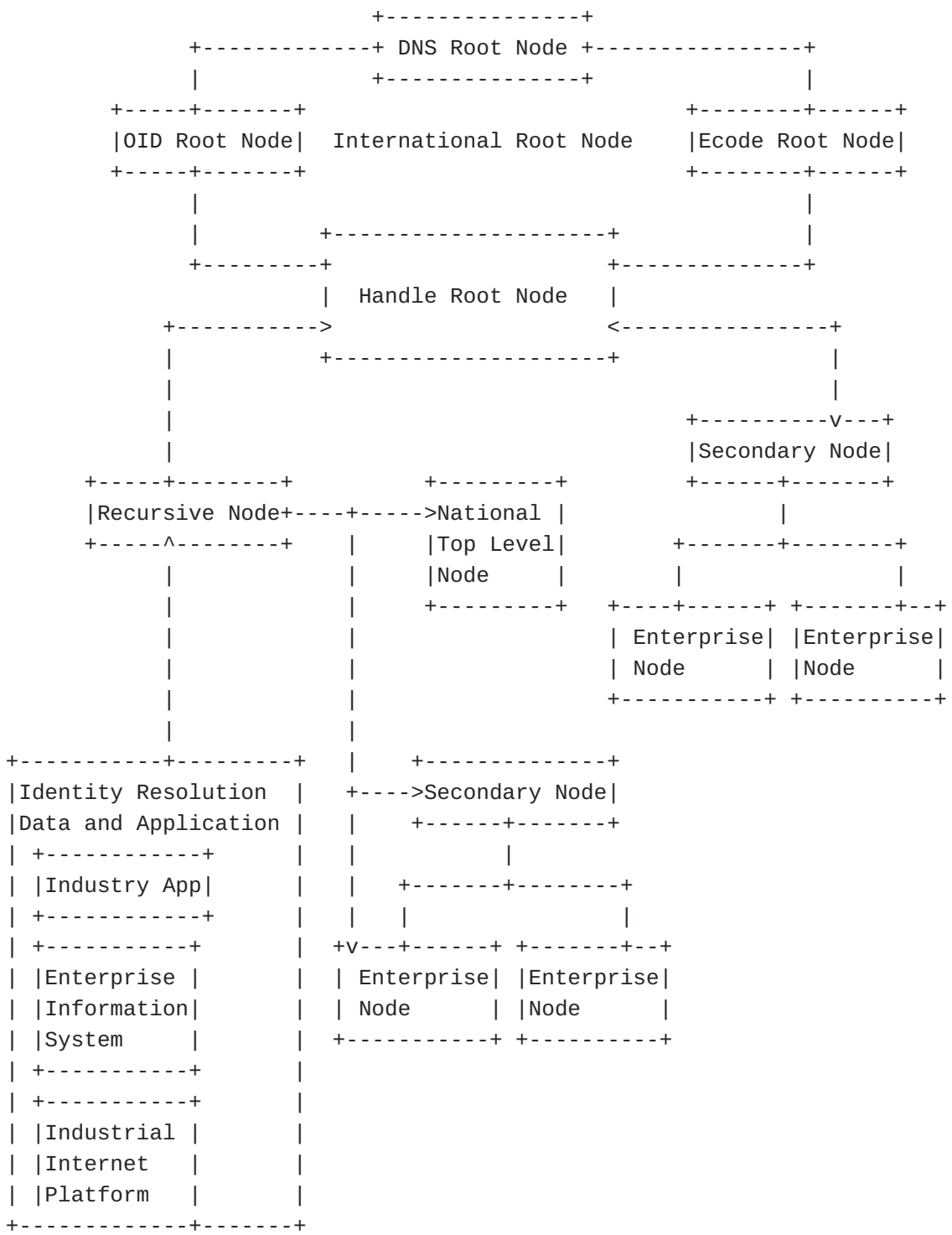

Figure 1: Industrial Internet Identity Resolution and Management Service System

6. Security Protection Scope

The security protection scope of the Industrial Internet identity resolution and management service system proposed in this draft mainly means that the identity is written into the device and is responsible for collecting product information, including device model, device type, generation batch, generation date, generation site, device production information link, device description data link, etc., integrate this information into identity data, and then publish it to the data exchange system for access by identity resolution enterprise nodes. Among the identity resolution enterprise node, the identity resolution secondary node, and the identity resolution root node, the process of data synchronization between the application scenarios, the collection of data transmission technologies used, is used to provide security assurance and security support for the Industrial Internet identity data transmission.

The scope of Industrial Internet identity data transmission security protection specifically includes the security and the security support of the data transmission interface within and between the functional domains of the Industrial Internet identity resolution system. Its role is in the whole life cycle of the system (planning and design, development and construction, operation and maintenance , abandonment and exit).

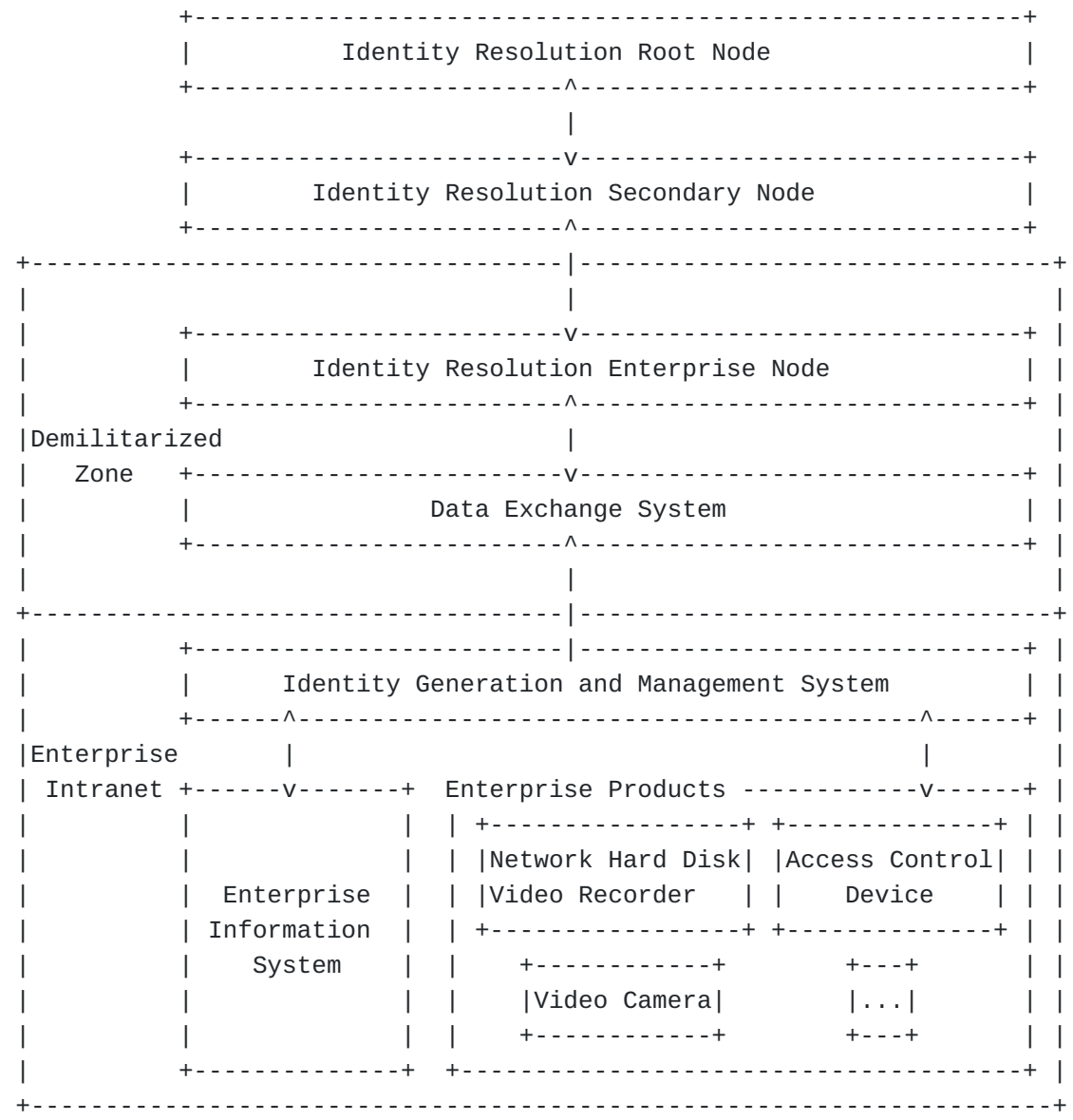

Figure 2: Industrial Internet Identity Resolution and Management Service System

7. Safety Technical Requirements

7.1. Data Transmission Integrity

Data transmission should comply with the following common requirements:

1) Support the information integrity check mechanism during transmission to realize the transmission integrity protection of management data, authentication information, sensitive information, important business data and other data (such as: check code, message abstract, digital signature, etc.).

2) Should have transmission delay and interrupt handling capabilities to ensure the integrity of the data.

3) Cryptographic technology should be used to protect the integrity of important data in transmit.

4) Measures should be taken to recover the data when data integrity is compromised.

7.2. Data Transmission Availability

The timeliness and accuracy of the data should be guaranteed during data transmission. Specifically:

1) Timeliness: the feature of identifying historical data received or data beyond the time limit. Specifically, the data comes from the system using a unified time allocation/correction mechanism, and the data should include time stamps, etc.

2) Accuracy: When there is an acceptable error in the data, there is an overload to ensure the normal acquisition of the data in time.

7.3. Data Transmission Confidentiality

When transferring data, it is necessary to ensure the confidentiality of the data, including:

1) For important data, authenticate information and important business data such as user passwords, biometrics, private keys, symmetric keys, product order information, and unique identity of a device (Handle ID), a certain strength encryption algorithm or other effective measures should be used to guarantee confidentiality.

2) Appropriate security protocols (such as HTTPS, SSH, IPSec, TLS, etc.) should be used to safeguard the data being transmitted.

7.4. Data Transmission Authentication

Ensure the legitimacy of the identities of both parties in the data transmission, which means, ensure the identity authentication of the subject to the object before the interaction, and establish a trusted transmission path.

7.5. Data Transmission Strategy

Establish a formal transmission strategy to protect the security of all types of information transmitted through communication facilities, and meet:

1) Clarify the type and scope of information that can be transmitted in plain text.

2) For sensitive data, such as user passwords, biometrics, private keys, symmetric keys, etc., an encrypted transmission strategy is required.

7.6. Data Transmission Protocol

The protocol should address the safe transmission of internal and external business, and meet:

Cryptographic algorithms such as data abstract, signature, and authentication shall use the cryptographic algorithms and combinations of abstract, signature, and authentication required by national regulations or national mandatory standards.

7.7. Maintenance and Update of Transmission Protocol

The confidentiality protocol for data transmission should be regularly maintained and updated so that the procotol should reflect the requirements for data transmission security protection and meet:

1) The transmission security protocol needs to be reviewed every year to ensure that the agreement should reflect the requirements for data transmission security protection

2) When new services are launched or existing services are changed, the transmission security protocol needs to be audited and updated if necessary

7.8. Log and Audit

The transmission system shall log and audit the following security failure events. The content of the log shall at least contains date/time, event type, event subject, event description, success/failure information, and meet the following requirements:

1) Data transmission establishment success and failure

2) Transmission device online monitoring abnormalities and alarm events

3) Malicious program intrusion alert event

4) Configuration modification operations caused by administrators/non-administrators

8. Security Considerations

This entire memo deals with security issues.

9. IANA Considerations

This documents has no IANA actions.

10. Informative References

[OID] "Introduction to OIDs and the OID Resolution System (ORS)", May 2020, <http://www.oid-info.com/introduction.htm>.

[RFC3650] Sun, S., Lannom, L., and B. Boesch, "Handle System Overview", DOI 10.17487/RFC3650, November 2003, <https://www.rfc-editor.org/info/rfc3650>.

[RFC3651] Sun, S., Reilly, S., and L. Lannom, "Handle System Namespace and Service Definition", DOI 10.17487/RFC3651, November 2003, <https://www.rfc-editor.org/info/rfc3651>.

Authors' Addresses

Bin Wang (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China

Phone: +86 571 8847 3644
Email: wbin2006@gmail.com

Kezhang Lin (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China

Phone: +86 571 8847 3644
Email: lkz_wz98@163.com

Chonghua Wang (editor)
IIE, CAS
Beijing
100093
China

Phone: +86 185 1894 5987
Email: chonghuaw@live.com

Xing Wang (editor)
Hikvision
555 Qianmo Road, Binjiang District
Hangzhou
310051
China

Phone: +86 571 8847 3644
Email: xing.wang.email@gmail.com