IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS REPORT

THE IEEE GLOBAL INITIATIVE ON TRUST TECHNOLOGY

THE DEVELOPMENT OF THE TRUSTED DIGITAL IDENTITY INDUSTRY IN FUTURE NETWORKS

Authored by

Lifeng Zhang and Yihui Zhang

IEEE

Documents
Document Sharing Hub

Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGMENTS

Special thanks are given to the following reviewers of this paper:

Ang Boon Chong
Chengkang Chu
Xueqin Jia
Tingting Liu
Bo Lv
Weizhi Meng
Yi Pan
Weiwei Pang
Long Shi
Xiaojia Song
Nina Wang
Yang Xiang
Liangliang Zhang
Yifeng Zhang
Hang Zhou
Jintao Zhu

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 30 October 2024. Printed in the United States of America.

PDF: STDVA27435 979-8-8557-1388-6

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

Copyright © 2024 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the ICCom members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Copyright © 2024 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks

TABLE OF CONTENTS

ABSTRACT 5

1. INTRODUCTION OF NETWORK IDENTITY 6

1.1. INTERNET NETWORK IDENTITY 6
1.2. COMMUNICATION NETWORK IDENTITY 7

FIGURE 1 EVOLUTION OF DIGITAL IDENTITY IN MOBILE COMMUNICATION NETWORKS 9

2. INSIGHTS INTO FUTURE NETWORK IDENTITY 9

2.1. THE INTEGRATION TREND 9
2.2. THE APPLICATION TREND 10
2.3. THE TECHNOLOGY TREND 12
2.4. THE INDUSTRY TREND 14
2.4.1. OVERVIEW 14
2.4.2. INTERNET-BASED FUTURE NETWORK IDENTITY 14
2.4.3. COMMUNICATION-BASED FUTURE NETWORK IDENTITY 15

3. THE TRUSTED DIGITAL IDENTITY 15

3.1. DEFINITION OF TRUSTED DIGITAL IDENTITY 15
3.2. KEY INDICATORS 16

4. FUTURE CONSIDERATIONS 18

4.1. DEVELOPMENT SUMMARY 18
4.2. TREND OUTLOOK 19

5. REFERENCES 20

Documents
Document Sharing Hub

Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks

THE DEVELOPMENT OF THE TRUSTED DIGITAL IDENTITY INDUSTRY IN FUTURE NETWORKS

ABSTRACT

As digitalization and intelligence advance, communication is expanding from the physical world to interactions between the physical and digital worlds. The focus is shifting from human-to-human to multi-modal interactions involving human-to-digital entities/robots and digital entity-to-digital entity communications. This shift necessitates new digital identity technologies, which are becoming crucial for establishing trust and connectivity between these worlds and supporting all digital activities.

With the advent of concepts like the next-generation internet (Web 3.0) and next-generation communication networks (6G), network identity is undergoing subtle changes, with trust emerging as a central element. Ensuring network security, simplifying access control and data encryption processes among multiple entities, and supporting the construction of an open, shared, and secure cyberspace community is essential. Additionally, pervasive cross-domain access requires trust endorsements for users' social attributes, and building a global trust framework using technologies like blockchain and distributed digital identities is crucial for enhancing the universality and extensibility of user credentials. Trust barriers between domains can be overcome with help from this framework, while users receive more flexible and cost-effective access options.

The historical development of information and communication network identity, as well as insights into network identity technologies, applications, and industry trends are reviewed in this report. Current approaches to implementing digital identity in future networks are outlined, and definitions and key metrics for trustworthy digital identities in future networks are proposed. Additionally, a forward-looking perspective on future developments is provided.

Copyright © 2024 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks

1. INTRODUCTION OF NETWORK IDENTITY

1.1. INTERNET NETWORK IDENTITY

The concept of trusted network digital identity has evolved alongside the development of communication technology (CT) and information technology (IT).

The native IT Internet Protocols (IPs) lack an identity layer, meaning that internet users do not have a native digital identity. When the internet was initially designed, it only provided identity identifiers for computer nodes, which were managed by centralized authoritative institutions. For example, the IEEE assigns Media Access Control (MAC) addresses to network devices, ensuring that each device has a unique hardware identifier. The Internet Assigned Numbers Authority (IANA) manages IP addresses, which are logical addresses used to identify devices on a network. The Internet Corporation for Assigned Names and Numbers (ICANN) manages domain names, converts user-friendly domain names into machine-readable IP addresses, and enables users to access resources on the internet. Additionally, the identity authentication of commercial websites is handled by certificate authorities (CAs). Since 1995, CAs have been issuing security certificates to ensure the security and trustworthiness of websites.

These organizations and protocols together form the basic patchwork of the internet's identity recognition and management system. While this ensures orderly network operation and secure information exchange, the internet has now become a global infrastructure operating in a fully open and complex environment. By December 2022, there were already 4.95 billion internet users worldwide (Ayed [1]).[1] However, the native Internet Protocols still lack a secondary confirmation mechanism in the communication network, where identity is verified through voice and real-time interactive information. With the rapid commercialization of the internet, relying on external forces and centralized management for security and trust is no longer feasible.

In particular, the next-generation internet (Web 3.0) emphasizes the concept of the *internet of value,* which involves economic activities such as e-commerce, data asset circulation, and digital asset exchanges. From an economic perspective, trust is fundamental to economic activities, and trusted identity is the foundation of all digital trust. Therefore, from the perspective of the internet, establishing a trusted digital identity is imperative.

[1] The numbers in brackets correspond to those of the references in Section 5.

Copyright © 2024 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks

1.2. COMMUNICATION NETWORK IDENTITY

The integration of communication network technology with digital identity technology has evolved. The first generation of mobile communication technology (1G) introduced digital identity technology to identify entities, though significant security vulnerabilities remained. For instance, 1G technology, represented by the Advanced Mobile Phone System (AMPS), was an analog cellular mobile communication system. However, within this system, users and devices were still assigned digital identifiers. Users were given a unique mobile identification number (MIN) by operators, while terminal devices were identified by an electronic serial number (ESN) assigned by manufacturers. When a user connected a terminal device to the communication network, the ESN and MIN were transmitted in plaintext. This led to widespread illegal phone cloning, posing major security risks affecting both users and operators.

The second generation of mobile communication technology (2G) pioneered the separation of device and Subscriber Identity Module (SIM) card identity, effectively reducing security risks. 2G technology, represented by Global System for Mobile Communications (GSM), introduced the innovative device-SIM separation approach, where a mobile phone and SIM card together formed the mobile communication terminal. This separation brought the following four key benefits:

- First, the SIM card provided storage for user data, including identity information and encryption keys. This allowed the GSM network to authenticate the user and encrypt voice data during calls, preventing phone cloning and eavesdropping.
- Second, it separated the identifiers for users, services, and devices. The international mobile equipment identity (IMEI) identified the terminal device, the international mobile subscriber identity (IMSI) stored on the SIM card uniquely identified the user for authentication, and the Mobile Station International ISDN Number (MSISDN) served as the service identifier for phone calls.
- Third, the introduction of SIM cards allowed users to replace lost SIM cards without affecting their phone numbers, as the IMSI would change but not the MSISDN.
- Fourth, it protected user privacy through the introduction of the Temporary Mobile Subscriber Identity (TMSI), which reduced the exposure of IMSI during transmissions over the air.

The third generation of mobile communication technology (3G) introduced mutual authentication capabilities and expanded service identifiers. 3G technology, represented by wideband code division multiple access

Copyright © 2024 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE The Development of The Trusted Digital Identity Industry In Future Networks