IEEE SA STANDARDS ASSOCIATION

This document contains supplemental information referenced by the European Rolling Plan for ICT Standardisation.

IEEE Standards Activities in the Network and Information Security (NIS) Space

Overview

IEEE has standardization activities in the network and information security space, and in anti-malware technologies, including in the encryption, fixed and removable storage, and hard copy devices areas, as well as applications of these technologies in smart grids.

IEEE's largest technical society, the IEEE Computer Society, is very well equipped to provide technical expertise in network and information security efforts. For over thirty years, the IEEE Computer Society has had a technical committee focused on computer security and privacy. It publishes the well-respected *IEEE Security & Privacy* magazine, which offers articles by top thinkers in the information security industry, and sponsors two long-established premier technical meetings: the IEEE Security and Privacy Symposium and the Computer Security Foundation Workshop.

Other IEEE societies such as the IEEE Communications Society, the IEEE Power and Energy Society, and the IEEE Engineering, Medicine, and Biology also have projects in security.

IEEE's Industry Connections Security Group (ICSG) is another important activity, providing a flexible and nimble platform for stakeholders to respond to the new malware environment. The ICSG has three key activities:

- The IEEE Anti-Malware Support Service (AMSS), a set of shared support services that enables the individual security companies and the industry as a whole to respond more effectively and efficiently to the rapidly mutating universe of contemporary malware threats. AMSS currently consists of two main services: the Clean file Metadata eXchange (CMX), and the Taggant System.
- The Malware Working Group, which develops better ways of sharing malware information, enabling the computer security industry to more effectively respond to malware threats. Current projects include SSL Man-in-the-Middle (MitM) and URL Brand Protection. While the former is designed to address problems with security software monitoring encrypted communications, the latter seeks to increase the effectiveness of anti-phishing solutions and reducing false positives.
- The Encrypted Traffic Inspection (ETI) Working Group, which is helping to develop an accepted way to inspect network traffic, on top of encrypted transport standards.

Relevant Standards Activities

It should be noted that some standards contain security aspects, but are not security standards. Those are not listed below. One notable example is the project P2413 - Standard for an Architectural Framework for the Internet of Things (IoT) which describes quadruple trust (protection, security, privacy, and safety).

Home and Local Area Network Security

Projects under Development

- IEEE 2900 - Standard for Smart Home Security: Overview and Architecture
- IEEE 2900.1 - Standard for Smart Home Security: Taxonomy and Definitions
- IEEE 802.1AE - IEEE Draft Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security
- IEEE 802.15.4y - Standard for Low-Rate Wireless Networks Amendment Defining Support for Advanced Encryption Standard (AES)-256 Encryption and Security Extensions

Encryption

Approved Standards*

- IEEE 1363-2000, IEEE Standard Specifications for Public-Key Cryptography
- IEEE 1363a-2004, IEEE Standard Specifications for Public-Key Cryptography--Amendment 1: Additional Techniques
- IEEE 1363.1-2008, IEEE Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices
- IEEE 1363.2-2008, IEEE Standard Specification for Password-Based Public Key Cryptographic Techniques
- IEEE 1363.3-2013, IEEE Standard for Identity-Based Cryptographic Techniques using Pairings

Secure Communications in Vehicular Environments

Approved Standards*

- IEEE 1609.2-2016, IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages
- IEEE 1609.2a-2017, IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages Amendment

Projects under Development*

- IEEE P1609.2.1, IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE) -- Certificate Management Interfaces for End-Entities
- IEEE P1609.2b, IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages Amendment

Fixed and Removable Storage

Approved Standards*

- IEEE 1619-2007, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
- IEEE 1619.1-2007, IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices
- IEEE 1619.2-2010, IEEE Standard for Wide-Block Encryption for Shared Storage Media
- IEEE 1667-2015, IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices

Security for Software Defined Networking and Network Function Virtualization

Projects under Development*

- IEEE P1915.1, Draft Standard for Software Defined Networking and Network Function Virtualization Security

Security for Hardcopy Devices

Approved Standards*

- IEEE 2600-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security
- IEEE 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A
- IEEE 2600.2-2009, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B
- IEEE 2600.3-2009, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment C
- IEEE 2600.4-2010, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment D

NIS for Smart Grid

Approved Standards*

- IEEE 1402-2000 (R2008), IEEE Guide for Electric Power Substation Physical and Electronic Security
- IEEE 1686-2013, IEEE Standard for Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE C37.240-2014, IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems

Projects under Development*

- IEEE P1711, Draft Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
- IEEE SA - 1711.2 - Standard for Secure SCADA Communications Protocol (SSCP)
- IEEE SA - 2030.102.1 - Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems

- IEEE SA - C37.249 - Guide for Categorizing Security Needs for Protection and Automation Related Data Files

Other domains
Projects under Development

- IEEE SA - 2721 - Standard for Wireless Health Device Security Assurance
- IEEE SA - 2025.2 - Standard for Consumer Drones: Privacy and Security
- IEEE SA - 1912 - Standard for Privacy and Security Architecture for Consumer Wireless Devices

**Draft standards projects, once approved, are often revised and/or used as the base for new projects. The status of these projects is updated periodically. For the most up-to-date status, please see the following link: <https://standards.ieee.org/project/index.html>*