CERTIFICATE SUPPLEMENT
EITCA/IS/ERF15004715

Certificate ID: EITCA/IS/ERF15004715
Certificate type: The European Information Technologies Certification Academy Programme
Academy name: EITCA Information Technologies Security Programme (EITCA/IS)
Issue date: December 2015
Holder's name: Artur Marek Maciag
Holder's country: Poland
Examination center: CompSecur Sp. z o.o., Wroclaw, Poland
Earned ECTS credits: 24

EITCA/IS Programme (version/revision: v1r1) component EITC Certificates:

Result:

EITC/IS/CF Cryptography fundamentals
EITC Certificate number: EITC/IS/CF/ERF/15004715

100%

Certificate Programme description: Introduction to cryptology, cryptography and cryptoanalysis: Basic definitions, Ciphering and deciphering techniques, Symmetrical and asymmetrical cryptosystems, Cryptographical algorithms classification, Authorization and authentication techniques, Methods of ensuring data integrity; Data privacy: history of symmetrical ciphers, Transposition ciphers, Substitution ciphers, Permutation and translation ciphers - matrices, Keys, XOR operation and modulo 2 bit-sum, Vernam cipher, One-time pad, Shannon's proof of OTP unconditional security, Credibility and authentication: Authentication techniques, Hash functions, MD5 implementation, Discrete logarithm, Pseudorandom sequences, Data integrity; Cryptology: cryptography, cryptoanalysis, Steganography, Cryptography formalization; Cryptosystems: asymmetrical, (public key cryptography, NP-difficult problems, asymmetrical algorithms, Public Key Infrastructure, PKI certification, digital signature), symmetrical (private key cryptography, algorithms, private key distribution, QKD - quantum cryptography); practical implementations of algorithms (symmetrical - Vernam cipher, DES, IDEA, RC5, 3DES, AES, Rijndael, NASZ; asymmetrical - RSA, Diffie-Hellman key distribution, El-Gamal); Authorization: Techniques of authorization and authentication (passwords, biometrical systems)
Certificate Programme version/revision: EITC/IS/CFv1r2

EITC/IS/SMMOS Security management in Microsoft operating systems
EITC Certificate number: EITC/IS/SMMOS/ERF/15004715

100%

Certificate Programme description: System installation: security aspects, installation of upgrades, patches and Service Packs; User accounts and authentication: User groups and privileges, Cooperation with strong authentication systems and their configuration; System and hardware devices configuration (printers): Plug&Play, Manual resources configuration; Network environment configuration: protocols (IP, TCP, UDP, etc.), Services (DHCP, DNS, WINS, LmHOSTS), Files and printers sharing, Build-in firewall, Remote access (Remote Desktop); Network domain configuration: Active Directory; IIS services configuration: Access rights, IIS services management, IIS servers (www server, ftp server), data sharing in Internet; Disk management: NTFS, disk quotas, security of data sharing, Data compression; Integrated system security, system restoration; System administration: MMC console; Backup and system restore points: registry files, System image; Critical situations: Recovery Console, NTFS partitions access, password recovery
Certificate Programme version/revision: EITC/IS/SMMOSv1r2

EITC/CN/SCN1 Computer networking 1
EITC Certificate number: EITC/CN/SCN1/ERF/15004715

71%

Certificate Programme description: Introduction to Network Communications; Paradigms of network communication: circuit switching, packets switching; Network topologies: ring, star, P2P, hybrid networks, network topologies at different layers; Network theory: Layer model of network communication, ISO/OSI reference model, Logical layers of communication (physical, data link, network, transport, session, presentation, application), TCP/IP protocol stack; Technologies and protocols of communication medium layer: standards of physical layer and data link layer (LAN networks and Ethernet standard, WAN networks, network devices in physical and data link layer (network adapters, repeaters, hubs, bridges, switches), Wireless LAN and MAN networks (Wi-Fi, WiMAX), Mobile networks (1G, 2G, 3G), Multiplexing techniques: CDMA, FDMA and others; Internet - network layer protocols (data encapsulation and transmission, IPv4 protocol and addressing, subnetworks and supernetworks, IPv6 protocol, IP-MAC projection, IP addresses and symbolical names - DNS, ICMP protocol; Internet - transport protocols, ports and sockets, UDP and TCP protocols, Application layer - network services: e-mail, SMTP, POP3 and IMAP protocols, File transfer - FTP and NFS protocols, information services - HTTP and NNTP protocols; Secure network protocols: SSL, IPsec, VPN private networks
Certificate Programme version/revision: EITC/CN/SCN1v1r2

EITC/IS/IST Information security theory
EITC Certificate number: EITC/IS/IST/ERF/15004715

71%

Certificate Programme description: Definition of information (classical state, message source): unit of information (bit) and other units of information, measures (Shannon entropy), Graph theory, Conditional probability, Bayes theorem; Random and pseudorandom sequences: importance of randomness to security; Introduction to coding: types of codes, Humming codes, compression (lossy and lossless), Shannon's Theorem; Communication channels: lossless channels, lossy channels, types of information noises, Error correction procedures; Basic definitions of information theory: algorithm, algebra, language, grammar; Computational complexity theory: classes of problems, polynomial problems (P), non-deterministic polynomial problems (NP), NP-complete problems, Context of asymmetrical cryptography; Computational models: state machines (Turing machine, DFA, NFA), Church-Turing Thesis; Boolean algebra and classical logical circuits theory: logical gates, universality, non-reversibility of binary information in Boolean algebra, implementations of algorithms; Probabilistic computational model: NBP problem class, extended Church-Turing Theorem; Quantum computational model: NQP problem class, Quantum circuits theory, Fundamental weakness of asymmetrical cryptography (Fourier transform, Shor's algorithm for factorization, Quantum Fourier transform by Kitaev, discrete logarithm problem, modulo algebra problem, hidden subgroup)
Certificate Programme version/revision: EITC/IS/ISTv1r2

This document is a formal attachment to issued certificate. All rights reserved. European IT Certification Institute, EITCI asbl, Brussels, Belgium, European Union

EITC/QI/QIF Quantum information and quantum computation fundamentals

78%

EITC Certificate number: EITC/QI/QIF/ERF/15004715

Certificate Programme description: Introduction to quantum mechanics: quantum information formalism (Hilbert space, norms and measures, wave functions, orthogonal and non-orthogonal vectors, ON basis, unitary and hermitian operators, spectral decomposition of operators, Dirac notation, introduction to functional analysis), Quantum mechanics postulates: quantum state, unitary evolution and SchrÃ¶dinger-Heisenberg equation, quantum measurement (von Neumann projection, Zurek's induced superselection), Tensor product and quantum entanglement; quantum paradigm of information: definition (information as quantum state, sources of information), Unit of information (qubit), Representation on Bloch sphere, Bell states, Measure of entanglement and quantum information (von Neumann entropy), Schmidt representation, Quantum measurement of qubits, EPR and basics of locality and realism: breaking the Bell inequality, Non-local correlations of measurement results, Quantum teleportation, Superdense coding, Quantum circuits theory: Quantum logical gates (one-qubit Pauli gates, Hadamard gates, phases, multi-qubit CNOT gates, Toffoli gates, Fredkin gates), Universal set (CNOT and one-qubit gates), Reversability of quantum information processing by unitarity of systems' evolution, Quantum algorithms implementation (implementation of quantum Fourier transform - exponential acceleration, implementation of quantum teleportation); Quantum security aspects: Shor's algorithm for factorization, no-cloning theorem, non-deleting and non-broadcasting theorem, Quantum Key Distribution; Practical realizations of quantum computer: decoherence, DiVincenzo criteria, trapped ions technology, NMR, Quantum dots (orbital and spin degrees of freedom), Quantum information over topological degrees of freedom
Certificate Programme version/revision: EITC/QI/QIFv1r2

EITC/IS/EEIS Electronic economy information security

71%

EITC Certificate number: EITC/IS/EEIS/ERF/15004715

Certificate Programme description: Information threats to electronic economy; Information security audit: analysis within organizations, Analysis of security of information flows, Auditing methods and tools, Threat model and STRIDE methodology; Threat mitigation: viruses, safe storage of data, Limiting network threats (firewalls, NAT, PAT, Proxy servers, IDS systems); Cryptographical data protection: Using cryptography for data security, Certification and public key infrastructure, Digital signature, SSL protocol, Virtual private networks, Network application and services security
Certificate Programme version/revision: EITC/IS/EEISv1r2

EITC/FC/CCT Computational complexity theory

85%

EITC Certificate number: EITC/FC/CCT/ERF/15004715

Certificate Programme description: Introduction to computational complexity theory; Calculation model based on Turing machine: formal definition, representation and language of Turing machine, recursive and recursively enumerable languages, Program definition and machine's state representation, machine's resource requirements, multi-track Turing machine, Non-deterministic Turing machine; Alternate models of complexity: RAM machine, instruction set, language recognition by RAM machine, Computational complexity in RAM model, comparison of time usage of RAM and Turing machines, Simulating the RAM machine by multi-track Turing machine, Comparison of memory complexity between computational models, Logical circuits; Computational complexity classes: Time and memory complexity classes, Linear acceleration and memory compression theories, Relations between classes, Savitch's theorem, class complements, Time and memory hierarchy theories; Reductions, Completeness and NP-complete problems: Polynomial and logarithmical reductions, polynomial transformation by Turing, NP class and NP-completeness (NP class in language of logic, existential 2-nd class statements and complexity, Fagin theorem), SAT, 3SAT, MAXSAT problems, NP-complete graph problems, Node cover, Clique, Independent set, Problems over sets and numbers (tripartite matching and set cover, subset sum and other numerical problems); Algorithms and approximation schemes: optimization and decision problems, Approximation solutions, greedy algorithms, MAX CUT problem, TSP problem, metric version, BIN PACKING, 2-approximation, KNAPSACK problem, Approximation schemes, L-reductions; Probabilistic algorithms: probabilistic complexity classes (ZPP, PP and BPP classes), prime numbers detection, Miller-Rabin test, Random bits generation, Models of concurrent calculations (PRAM), Classes in PRAM models, P-completeness, Concurrency and randomization; Function problems and computational complexity: FP, FNP and TFNP classes, #P class, Valiant theorem, Parity-P class; Logarithmical memory, polynomial hierarchy, polynomial memory and exponential complexity: L, NL and coNL classes, Immerman-SzelepcsÃ©nyi theorem, coNP and DP classes, Alternating machines, PSPACE class, PSPACE-complete problems (periodical optimization), Regular expressions; Cryptography and complexity: one-way functions
Certificate Programme version/revision: EITC/FC/CCTv1r2

EITC/IS/QCF Quantum cryptography fundamentals

65%

EITC Certificate number: EITC/IS/QCF/ERF/15004715

Certificate Programme description: Classical approach to secure information communication: general idea of secure communication channels, private key cryptography, public key cryptography, authentication, noisy channels (errors detection, errors correction, errors detection and correction in Ethernet networks), weaknesses of classical cryptography; Unconditionally secure quantum channels conception (unconditional security of communication, Vernam cipher, One-Time-Pad cryptosystem); Quantum information: fundamental quantum information principles and postulates (definition of the qubit, the No-Cloning theorem), quantum information processing in practice; Quantum Mechanics applications towards protection of classical information; Quantum Key Distribution without use of entanglement: fundamental properties of polarized photons, Bennett and Brassard BB84 protocol, Bennett B92 protocol, Quantum Key Distribution with use of entanglement: quantum entanglement and quantum measurement outcomes correlations, EPR paradox, Bell inequalities violation, CHSH inequality violation, entanglement based Ekert E91 protocol; QKD secured communication channels: potential attacks on the quantum key distribution scheme, quantum channels with noise, privacy amplification (PA), authentication, complete scheme of secure communication, theoretical security analysis and assessment; Practical quantum cryptography implementations: QKD systems prototypes (MagiQ, idQuantique), DARPA quantum network (network structure, implementing technologies, software network layer, IPsec protocol extensions towards integration with the QKD by means of IKE implementation), European Framework Programme SECOQC project (integration of different QKD technological implementations), standardization, commercial solutions and their applications; Other applications of quantum mechanics in cryptography: bit commitment and quantum coin tossing, quantum random numbers generators, alternative ways of implementing eavesdropping proof communication channels (Kish protocol), future and perspectives of quantum cryptography
Certificate Programme version/revision: EITC/IS/QCFv1r2

This document is a formal attachment to issued certificate. All rights reserved. European IT Certification Institute, EITCI asbl, Brussels, Belgium, European Union

EITC/CN/SCN2 Computer networking 2

78%

EITC Certificate number: EITC/CN/SCN2/ERF/15004715

Certificate Programme description: Ethernet: operations basics, Ethernet frames, MAC protocol (CSMA/CD protocol, transmission errors, work mode negotiation), Ethernet system structure, repeaters, hubs, bridges, switches, network connection redundancy; Communication media: electric wires, twisted-pair cables, concentric cable, copper wire categories, UTP wire based networks, Optical fibres (single-mode and multi-mode optical fibres, optical fibre connectors), WLAN networks, Connectivity over radio frequencies, basic elements of wireless networks, advantages of wireless networks, 802.11 standards, WLAN security, WEP, TKIP, WPA, 802.1X, NAC, WAN networks: Frame Relay (Frame Relay in OSI model, frame error detection, typical infrastructure of FR network, FR frame structure, logical connections in FR, correlation of data transmission in channels and CIR and EIR values, overload control, Audio/Video data in FR networks, LMI protocol), Asynchronous Transfer Mode (ATM devices, ATM addresses, types of connections, cell structure, model of ATM network, ATM interfaces, ILMI protocol, PNNI protocol), ATM and computer networks (LANE standard, ATM connections in LANE 1.0, LANE 2.0, IP over ATM); IP address acquisition: ARP protocol, BOOTP protocol, DHCP protocol; DNS: history, structure and operation of DNS, name structure, DNS servers, IP routing: static routing, dynamic routing (division based on area of operations, based on routing method, dynamic routing protocol examples, requirements for routing protocols, routing metrics, RIPv1 and RIPv2 protocols, avoiding routing loops, OSPF protocol, EIGRRP protocol)
Certificate Programme version/revision: EITC/CN/SCN2v1r2

EITC/IS/OS Operating systems security

100%

EITC Certificate number: EITC/IS/OS/ERF/15004715

Certificate Programme description: Introduction to operating systems: classification of operating systems (based on methods of processing, number of executed commands or number of users, other types of operating systems), principles of functioning of operating systems (instruction execution cycle, interrupts, memory protection, clock interruption); processes, resources, threads: process and resource handling (types of system core compilation in process and resource management, managers, cycle of states and processes changes, resource classification, process queues, context switching, basic operations on processes and resources), threads (thread implementation, thread context switching, basic operations on threads), thread and process implementation in Linux and Windows; file system - logical layer: files in operating system (operating system's tasks, file attributes, file types, file structure, methods of file access, basic operations on files), file access interface in unix-like systems, logical organization of file system (zones, operations on catalogs, catalog logical structure); file system - physical layer: disk space assignment (continuous assignment, list assignment, chain assignment, index assignment), free space management, catalog implementation, cache storage in file system, file system integrity, file access synchronization; file system - overview of implementations (CP/M, MS DOS and Windows 9x [FAT12/16/32], ISO 9660, UNIX, NTFS); importance of security, security threats, general problems of security, security strategy, security policies, security management paradigms and norms; basic problems of operating systems' security: introduction, security breaches, determining the operating system of attacked computer, authentication, resource access rights (standards: POSIX 1003.1, POSIX 1003.1e/1003.2c, access lists - ACL), special permissions in Unix, malware (viruses and bugs), masked communication channels; authentication and access control: general principles of authentication in Linux, file access rights in Unix-like systems, POSIX ACL mechanism in Windows and Linux (local access control in Linux and MS Windows), modular authentication and access control systems - RAM mechanism; permissions' limitation and delegation, trust domains, remote access control: controlled application execution environment, controlled layers of server operating systems, permissions delegation (limits mechanism, SUDO mechanism, SUID and SGID mechanisms), mechanisms of remote access control (usage of trust domains, rlogin command in Linux, securing network services with tcpd); operating system security amplification in MS Windows network environments: user accounts, file system, data encryption (encryption on file system level, data archives with cryptographical protection, e-mail cryptographical protection), network environment (network neighbourhood and network shares, hiding the computer in network, network connections, network firewalls)
Certificate Programme version/revision: EITC/IS/OSv1r2

EITC/IS/ACNS Advanced computer networks security

71%

EITC Certificate number: EITC/IS/ACNS/ERF/15004715

Certificate Programme description: Fundamental problems of computer networks security: network layer, transport layer, application layer, typical attacks on network infrastructures, Denial of Service attacks (review of DoS attacks, defensive methods against DoS/DDoS attacks), remote access security mechanisms, security tools; VPN virtual tunnels: configuration of VPN networks, IPsec protocol (IPsec protocol working modes, Authentication Header AH protocol, ESP protocol, security association, key management, protocol limits, IPsec in Windows Operating System, security of IPv6 protocol), port forwarding and application connections propagation, SSL tunnels; Firewalls and network address translation, functions of firewall systems, components of firewall systems (filtering router, computer fortress, demilitarized zone), network address translation (NAT), additional functionalities of firewalls,problems in firewalls implementation; Attack methods on WWW applications, countermeasures and defensive techniques: stealing of the source code, hidden HTML fields, Cookies variables, Path Traversal, SQL Injection, session takeover, software firewalls systems, software Intrusion Detection Systems IDS: software firewall implementations, netfilter/iptables networks firewall (iptables configuration, address translation, iptables extension modules, short target descriptions TARGETs, additional informations, examples), built-in personal firewall in Microsoft Windows Operating Systems, Intrusion Detection Systems IDS, Snort system, Secure configuration of the Apache HTTP server: introduction, Apache server, log of the Apache server, logical and physical paths, block directives, remote access security based on addresses, access control by user authorization, HTTPS connections; VPN networks in Linux and MS Windows environment: applications of the VPN technology, creation of VPN networks in Linux and Windows, OpenVPN software (fundamentals of operation, VPN Linux to Linux connection with use of the shared key method, VPN Linux to Linux connection with use of the digital certificates method, VPN Linux to Windows connection with use of the shared key method, summary of the OpenVPN software functionalities), Openswan software package (IPsec protocol implementation, VPN creation by use of the Openswan software); spoofing: types and methods of the spoofing attacks (IP spoofing, web spoofing, e-mail spoofing, DNS spoofing, Caller ID spoofing, SMS spoofing)
Certificate Programme version/revision: EITC/IS/ACNSv1r2

EITC/IS/FAIS Formal aspects of information security

100%

EITC Certificate number: EITC/IS/FAIS/ERF/15004715

Certificate Programme description: Introduction to information security, threats and risks: classification of information security and threats, norms and security policies, standards and norms, ITIL, BS 15000, ISO/IEC 20000, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002:2005, Basel I, Basel II, BS 7799-1, BS 7799-2, BS 7799-3:2006, ISO/IEC 17799:2005, D GINB recommendation, TISM methodic, OSSTM methodic, PAS-56, PAS-77:2006, PAS 99 :2006, BS 25999, ISO 28000 - supply chain security management, COSO, COSO II, SOX, COBIT, ISO/IEC TR 18044, ISO/IEC 24762:2008, ISO/IEC 15408, ISO/IEC TR 13335, ISO 19011:2002, PN-I- 02000:2002, ISO Guide 73:2002; legal aspects, legal acts on the protection of personal data, legal acts on public statistics, legal acts on fighting unfair competition, legal acts on electronic payment instruments, criminal law and Penal Code, legal acts on classified information protection, legal acts on telecommunications, legal acts on electronic banking, legal acts on archiving and national archives, legal acts on computerization of public administration entities, legal acts on electronic services provision, legal acts on citizens and property protection, legal acts on electronic signatures, legal acts on data bases protection, legal acts on copyrights and related authorship law; Software licensing models: EULA, GNU project, Gnu's Not Unix! (free software, copyleft, Free Software Foundation, GNU/Linux, free documentation, Open Source, GNU GPL license, GFDL license), other types of licenses (BSD license, X11 license, Linux type license, Public Domain license, Demo license, Freeware license, Shareware license, group license, Adware license, Firmware license, OEM license, MOLP license, BOX license); information security audit: rules of secure IT systems design, STRIDE

This document is a formal attachment to issued certificate. All rights reserved. European IT Certification Institute, EITCI asbl, Brussels, Belgium, European Union

model (fundamental idea, Data Flow Diagrams, design of threats model in STRIDE methodology)
Certificate Programme version/revision: EITC/IS/FAISv1r1

EUROPEAN IT CERTIFICATION INSTITUTE · ASBL · BRUSSELS · EU ·