



# CIPSEC Glossary

WP1, WP2, WP3 and WP5

## CIPSEC

### Enhancing Critical Infrastructure Protection with innovative SECurity framework

Due date: 30-04-2018  
Actual submission date:  
© CIPSEC Consortium

|  |              |            |                                 |               |
|--|--------------|------------|---------------------------------|---------------|
| <b>HORIZON 2020. WORK PROGRAMME 2014 – 2015</b>                              |              |            | Project No                      | 700378        |
| <b>Call</b>  |              |            | Instrument action               | Innovation    |
| Digital Security: Cybersecurity, Privacy and Trust                           |              |            | Start date                      | May 1st, 2016 |
| Secure societies. Protecting freedom and security of Europe and its citizens |              |            | Duration                        | 36 months     |
| DS-03-2015: The role of ICT in Critical Infrastructure Protection            |              |            | Website                         | www.cipsec.eu |
| <b>Public</b>  | Confidential | Classified | Lead contractor Atos SPAIN S.A. |               |

The research leading to these results has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700378.

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

The opinions expressed and arguments employed in this document do not necessarily reflect the official views of the Research Executive Agency (REA) or the European Commission.

This deliverable has been endorsed by Security Advisory Board.

## Document contributors

| Editor                                 | UPC    |
|--|--------|
| <b>Contributors</b>                    |        |
| Ilias Spais, Vassilis Prevelakis       | AEGIS  |
| Antonio Álvarez                        | ATOS   |
|  | BD     |
| Yael Chapal, Gil Cohen                 | COMSEC |
| Vittorio Vallero, Barbara Lumel        | CSI    |
| Dominik Renkel                         | DB     |
| Panos Pangiontis                       | EMP    |
| Leonidas Kallipolitis, Manos Athanatos | FORTH  |
| Manel Sanz                             | HCPB   |
|  | TUD    |
| Eva Marín Tordera, Sarang Kahzadaveh   | UPC    |
| Apostolos Fournaris                    | UOP    |
| Denis Guilhot, Francisco Hernández     | WOS    |

## Document history

| Version | Date       | Author  | Notes                         |
|---------|------------|---|-------------------------------|
| 0.0     | 16-2-2018  | Sarang Kahzadaveh   | 1 <sup>st</sup> Excel version |
| 0.1     | 28-03-2018 | Eva Marín Tordera   | 2 <sup>nd</sup> Excel version |
| 1.0     | 17-4-2018  | Eva Marín Tordera, Ilias Spais, Vassilis Prevelakis, Yael Chapal, Gil Cohen, Vittorio Vallero, Barbara Lumel, Dominik Renkel, Panos Pangiontis, Leonidas Kallipolitis, Manos Athanatos, Manel Sanz, Apostolos Fournaris, Denis Guilhot, Francisco Hernández | Last Excel version            |
| 1.0     | 24-4-2018  | Eva Marín Tordera   | 1 <sup>st</sup> Word version  |

## Deliverables

This glossary gathers all the acronyms in the submitted deliverables until month M18:

- D1.1 CI base security characteristics and market analysis report
- D1.2 Report on functionality building blocks
- D1.3 Report on taxonomy of the CI environments
- D2.1 CIPSEC System design
- D2.2 CIPSEC Unified Architecture – First Internal Release
- D2.3 CIPSEC products integration on the Unified Architecture
- D2.4 CIPSEC services integration on the Unified Architecture
- D3.1 Preliminary Pilot I Integration: Incident Discovery and Response for Railway use case
- D3.2 Preliminary Pilot II Integration: Hospital’s Operational Technology Management System use case
- D3.3 Preliminary Pilot III Integration: Air quality Monitoring System use case.
- D3.4 CIPSEC Intra/Interdependencies Analysis Preliminary Report
- D5.1 Dissemination plan and market analysis
- D5.2 CIPSEC annual report on exploitation, dissemination and standardization (Year 1)

## CIPSEC Glossary

|                 |  |
|-----------------|--|
| AAA             | Authentication, Authorization and Accounting   |
| ACH             | Automated Clearing Houses  |
| ACL             | Access Control List  |
| AD              | Analogical Digital   |
| ADC             | Application Defense Center   |
| ADSL            | Asymmetric Digital Subscriber ILne   |
| AES             | Advanced Encryption Standard   |
| AG              | AktienGesellschaft (a company which can be traded at stock exchange)                             |
| AgID            | Agency for Digital Italy   |
| ALG             | Application Level Gateway  |
| AMX controllers | Control module of the AMX company<br><a href="https://www.amx.com/en">https://www.amx.com/en</a> |
| API             | Application Programming Interface  |
| APN             | Access Point Name  |
| APS             | Access Points  |
| ApT             | Advanced Persistent Threat   |
| APT             | Advanced Packaging Tool  |

|              |  |
|--------------|--|
| AQDRS        | Air Quality Detection Regional System  |
| ARC-C        | ARc in C, mobile x-ray system in form of arc   |
| ARP          | Address Resolution Protocol  |
| ARPA         | Agenzia Regionale per la Protezione Ambientale (Regional Agency for the Environmental protection)  |
| ASIC         | Application Specific Integrated Circuit  |
| ASM          | Application Security Manager   |
| ATM          | Automated Teller Machine   |
| ATP          | Advanced Threat Protection   |
| AV services  | AudioVisual services   |
| AVT          | AEGIS Visualization Toolkit  |
| AWWA         | American Water Works Association   |
| AXIS modules | Control module of the AXIS company<br><a href="https://www.axis.com/es-es">https://www.axis.com/es-es</a>  |
| Az           | Axle Counter   |
| BCP          | Business Continuity Plan   |
| BETTERCARE   | Software platform that captures biomedical signals from a wide range of medical devices<br><a href="http://bettercare.es/">http://bettercare.es/</a> |
| BLAKE2       | It is a cryptographic hash function  |
| BLAS         | Basic Linear Algebra Subprogram  |
| BLE          | BlueTooth Low Energy   |
| BMC          | Business Model Canvas  |
| BRAINLAB     | Medical Technology Company<br><a href="https://www.brainlab.com/es/acerca-de-brainlab/">https://www.brainlab.com/es/acerca-de-brainlab/</a>          |
| BSI          | Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Security in Information Technology)  |
| BT           | Bluetooth Low Energy   |
| BÜSA-FSÜ     | Railroad Crossing with driveway control  |
| BYOD         | Bring Your Own Device  |
| C.A.P.S.E    | Consorti d'Atenció Primària de Salut de l'Eixample (Consortium of Primary Health Care of the Eixample)   |
| CAST-128     | It is a cypher, CAST stands for Carlisle Adams and Stafford Tavares  |

|         |  |
|---------|--|
| CATO    | Corporate Account Take Over  |
| CBC     | AES Cipher Block Chaining Mode   |
| CCID    | Chip Card Interface Device   |
| CCS     | Command and Control System   |
| CCTV    | Closed-Circuit Television Systems  |
| CD      | Compact Disc   |
| CDA     | Clinical Document Architecture   |
| CDC     | Communications Device Class  |
| CDN     | Content Delivery Network / Content Distribution Network  |
| CEK     | Centre Esther Koplovic (Esther Koplovic Center)  |
| CEN     | European Committee for Standardization   |
| CEP     | Complex Event Processing   |
| CERT    | Cyber Emergency Response Team  |
| CHAP    | Challenge-Handshake Authentication Protocol  |
| CI      | Critical Infrastructure  |
| CIO     | Chief Information Officer  |
| CIP     | Critical Infrastructure Protection   |
| CIPI    | Critical Infrastructure Performance Indicator  |
| CIs     | Critical Infrastructures   |
| CISO    | Chief Information Security Officer   |
| CLC     | CIPSEC Cloud   |
| CLI     | Command Line Interface.  |
| CNPIC   | National Centre for the Protection of Critical Infrastructures   |
| CO2     | Carbon Dioxide   |
| COEX    | Medical building   |
| Conduit | Communication between zones according to IEC 62443,<br><a href="https://en.wikipedia.org/wiki/Cyber_security_standards#ISA/IEC-62443_(formerly_ISA-99)">https://en.wikipedia.org/wiki/Cyber_security_standards#ISA/IEC-62443_(formerly_ISA-99)</a> |
| COP     | Centro Operativo Provinciale (Provincial Operation Centre)   |
| COTS    | Commercial Off-The-Shelf   |
| CPD     | Centre of Data Processing  |
| CPU     | Central Processing Unit  |

|        |  |
|--------|--|
| CSET   | Cyber Security Evaluation Tool   |
| CSI    | ConSortium for Information systems Piemonte  |
| CSIRT  | Computer Security Incident Response Team   |
| CSRF   | Cross-Site Request Forgery   |
| CSSP   | Control Systems Security Program   |
| CSV    | Comma Separated Values   |
| CSWG   | Cyber Security Working Group   |
| CT     | Computed Tomography  |
| CTR    | Counter Mode   |
| D      | Deliverable  |
| D3JS   | Data Driven Documents JS, It is a JavaScript library   |
| DB     | Data Base  |
| DCS    | Distributed Control System   |
| DDoS   | Distributed Denial of Service  |
| DER    | Distributed Energy Resources   |
| DES    | Data Encryption Standard, It is a cyphering algorithm  |
| DHS    | Department of Homeland Security  |
| DICOM  | Digital Imaging and Communication in Medicine  |
| DLP    | Data Leak Protection / Data Loss Prevention  |
| DMZ    | Demilitarized Zone (referred to as a perimeter network)  |
| DNA    | Deoxyribonucleic Acid  |
| DNP3   | Distributed Network Protocol   |
| DNS    | Domain Name Server   |
| DoCu   | Documentation System   |
| DoD    | US Department of Defense   |
| DORLET | Company complete security solutions<br><a href="https://www.dorlet.com/">https://www.dorlet.com/</a> |
| DoS    | Denial of Service Attack   |
| DR     | Disaster Recovery  |
| DRP    | Disaster Recovery Plan   |
| DSA    | Digital Signature Algorithm  |
| DTCC   | Depository Trust & Clearing Corporation  |

|          |   |
|----------|---|
| DuQu     | It is a collection of computer malware thought to be related to the Stuxnet worm<br><a href="https://en.wikipedia.org/wiki/Duqu">https://en.wikipedia.org/wiki/Duqu</a> |
| DVD      | Digital Video Disc  |
| DVR      | Digital Video Recorder  |
| EA       | Input/Output Subsystem  |
| EAP-TTLS | Extensible Authentication Protocol - Tunneled Transport Layer Security  |
| EBA      | Eisenbahn Bundesamt (National Railway Safety Authority)   |
| EBD      | EisenBahnbetriebsfeld Darmstadt (Testing facility of DB)<br><a href="http://www.eisenbahnbetriebsfeld.de/">http://www.eisenbahnbetriebsfeld.de/</a>                     |
| ECC      | Elliptic Curve Cryptography   |
| ECDH     | Elliptic Curve Diffie-Hellman   |
| ECDHE    | Elliptic Curve Diffie-Hellman Ephemeral   |
| ECDSA    | Elliptic Curve Digital Signature Algorithm  |
| ECFHMQV  | Elliptic Curve Fully Hashed Menezes Qu Vanstone, t is a variation of the ECMQV (Elliptic Curve Menezes Qu Vanstone)   |
| ECG      | Electrocardiographs   |
| EC       | European Commission   |
| ECI      | European Critical Infrastructures   |
| ECIES    | Elliptic Curve Integrated Encryption Scheme   |
| ECMQV    | EC Menezes Qu Vanstone  |
| ECSO     | European Cyber Security Organisation  |
| EDR      | Event Data Recorder   |
| EEPROM   | Electrically Erasable Programmable Read-Only Memory   |
| EFS      | Encrypting File System  |
| EGA      | Anesthetic Gas Extraction   |
| EHR      | Electronic Health Record  |
| EIDAS    | European Parliament and Council Regulation  |
| eIDAS    | electronic IDentification, Authentication and trust Services  |
| ENISA    | European Union Agency for Network and Information Security  |
| EOS      | European Organization of Security   |
| EPCIP    | European Program for Critical Infrastructures Protection  |

|         |   |
|---------|---|
| EPL     | Event Processing Language   |
| ERNICIP | European Reference Network for Critical Infrastructure Protection               |
| ERP     | Enterprise Resource Planning  |
| ESP     | Event Stream Processing   |
| ESTW    | Electronic interlocking system  |
| ESTW/ZE | Electronic Interlocking – Central Unit  |
| ETCS    | European Train Control System   |
| ETCS-Z  | European Train Control System – Central Unit                                    |
| ETL     | Extract, Transform and Load   |
| ETSI    | European Telecommunications Standards Institute                                 |
| EU      | European Union  |
| EULYNX  | European Initiative. Linking Interlocking Subsystems                            |
| f2f     | Face to Face  |
| FDE     | Full Disk Encryption  |
| FEA     | Field Element Area  |
| FeAK    | Field Element Junction Box  |
| FFIEC   | Federal Financial Institution Examination Council                               |
| FI      | Financial Institutions  |
| FIA     | Fault Injection Analysis  |
| FLC     | Laminar Flow Cabinet  |
| FPGA    | Field-Programmable Gate Array   |
| FQDN    | Fully Qualified Domain Name   |
| FR      | Foundational Requirement  |
| FS-ISAC | Financial Services Information and Sharing Center                               |
| FW      | Firewall  |
| GCM     | Galois Counter Mode   |
| GDPR    | General Data Protection Regulation  |
| GGM     | It is a pseudorandom generator, GGM stands for Goldreich, Goldwasser and Micali |
| GO      | Governmental Organizations  |
| GOST    | Gosudarstvenny Standardt (Group of standards developed in the USSR)             |



|           |  |
|-----------|--|
| GP        | (Alaris GP) Model of pump<br><a href="https://www.bd.com/es-es/our-products/infusion/infusion-devices/alaris-plus-platform-with-guardrails-safety-software/alaris-gp-plus-volumetric-pump-with-guardrails">https://www.bd.com/es-es/our-products/infusion/infusion-devices/alaris-plus-platform-with-guardrails-safety-software/alaris-gp-plus-volumetric-pump-with-guardrails</a> |
| GPRS      | General Packet Radio Service   |
| GPS       | Global Positioning System  |
| GSM       | Global System for Mobile Communications  |
| GSM-R     | Global System for Mobile Communications-Railway  |
| GWT       | Google Web toolkit   |
| HCB       | Hospital Clinic de Barcelona   |
| HD        | Hard Disk  |
| HDFS      | Hadoop Distributed File System   |
| HDMI      | High-Definition Multimedia Interface   |
| HD-SDI    | High Definition Serial Digital Interface   |
| HID       | Human Interface Device   |
| HIDS      | Host-based Intrusion Detection Systems   |
| HIPAA     | Health Insurance Portability and Accountability Act  |
| HIPS      | Host Intrusion Prevention System   |
| HIS       | Hospital Information System  |
| HL7       | Health Level-7 refers to a set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers  |
| HMAC      | Keyed-hash Message Authentication Code, is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key.  |
| HMI       | Human-Machine Interface  |
| HSM       | Hardware Security Module   |
| HTTP      | Hypertext Transfer Protocol  |
| HTTPS     | Secure Hypertext Transfer Protocol   |
| HVAC      | Heating, Ventilation and Air Conditioning  |
| HW        | Hardware   |
| HW and SW | Hardware and Software  |
| I/O       | Input/Output   |

|       |   |
|-------|---|
| IBI   | Industrial Business Intelligence  |
| ICS   | Industrial Control Systems  |
| ICyS  | Industrial Cyber security   |
| ICT   | Information and Communication Technology  |
| ICTC  | Information and Communications Technology Council   |
| ICTCP | ICT Contingency Plan  |
| ICTs  | Information and Communication Technologies  |
| ICU   | Intensive Care Unit   |
| ID    | Identification, Identity  |
| IDEA  | International Data Encryption Algorithm   |
| IDS   | Intrusion Detection Systems   |
| IED   | Improvise Explosive Device  |
| IED   | Intelligent Electronic Devices<br><br><a href="https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid">https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ict-inderdependencies-of-the-smart-grid</a> |
| IETF  | Internet Engineering Task Force   |
| ILS   | InterLocking System   |
| IMS   | IP Multimedia core network Subsystems   |
| IOC   | Indicator Of Compromise   |
| IODEF | Incident Object Description Exchange Format   |
| iOS   | Integrated Operating System (which integrates the operator station and telecommunication equipment)   |
| IoT   | Internet of Things  |
| IP    | Internet Protocol   |
| IPS   | Intrusion Prevention System   |
| IPSEC | Internet Protocol Security  |
| ISA   | International Standard Atmosphere   |
| ISAO  | Information Sharing & Analysis Organizations  |
| ISCOM | Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Higher Institute of Communications and Information Technologies)   |
| ISCPA | Cyber Security Protection Alliance  |
| ISDN  | Integrated Services Digital Network   |

|       |  |
|-------|--|
| ISMS  | Information Security Management System   |
| ISO   | International Organization for Standardization   |
| ISP   | Internet Service Provider  |
| IT    | Information Technology   |
| IT/OT | Information technology/Operation technology  |
| ITSG  | IT-Sicherheitsgesetz (IT-Security Law in Germany)  |
| ITU   | International Telecommunication Union  |
| JDBC  | Java DataBase Connectivity   |
| JNI   | Java Native Interface  |
| JNR   | Jammer to Noise Ratio  |
| JRI   | It is a company which develops monitoring systems for temperature, humidity and other physical parameters<br><br><a href="http://www.jri.fr/en/">http://www.jri.fr/en/</a> |
| JSON  | JavaScript Object Notation   |
| KISA  | Communication Infrastructure for safety-relevant Applications  |
| KPI   | Key Performance Indicator  |
| KVM   | Kernel-based Virtual Machine   |
| LAN   | Local Area Network   |
| LDAP  | Lightweight Directory Access Protocol  |
| LED   | Light Emitting Diode   |
| LEU   | Lineside Electronic Unit   |
| LIM   | Rack of telephone extensions   |
| LMS   | Learning Management System   |
| LoRa  | Low Range, low power wireless technology   |
| LS    | Light Signal   |
| LST   | Leit- und Sicherungstechnik (Command and Control System)   |
| LTE   | Long Term Evolution  |
| LUC   | Local Update Component   |
| M     | Month  |
| M2M   | Machine To Machine   |
| MAC   | Media Access Control   |
| MBR   | Master Boot Record   |

|            |   |
|------------|---|
| MCU        | Multipoint Control Unit   |
| MD2        | Message-Digest Algorithm 2, <a href="https://en.wikipedia.org/wiki/MD2_(cryptography)">https://en.wikipedia.org/wiki/MD2_(cryptography)</a>   |
| MD4        | Message-Digest Algorithm 4<br><a href="https://en.wikipedia.org/wiki/MD4">https://en.wikipedia.org/wiki/MD4</a>   |
| MD5        | Message-Digest Algorithm 5<br><a href="https://en.wikipedia.org/wiki/MD5">https://en.wikipedia.org/wiki/MD5</a><br><br>The MD2, MD4 and MD5 algorithms are hash functions that calculate a digest of a message so as to provide integrity. The numbers indicate the version of the MD |
| MDAV       | Maximum Distance to Average Vector  |
| MDC2       | Modification Detection Code 2, Cryptographic hash function  |
| MdM        | Mobile device Management  |
| MDM        | Maintenance and Data Management   |
| MES        | Management Execution Systems  |
| MIK        | Module Identity Key   |
| MRI        | Magnetic Resonance Imaging  |
| MSC        | Mass Storage Class  |
| MSCHAP     | Microsoft Challenge Handshake Authentication Protocol   |
| MTD        | Maximum Tolerable Downtime  |
| MVP        | Minimum Viable Product  |
| NAC        | Network Access Control  |
| NAS        | Network Access Storage  |
| NAT        | Network Address Translation   |
| NBAD       | Network Behaviour Anomaly Detection   |
| NCSS       | National Cyber Security Strategy  |
| NERC       | North American Electric Reliability Corporation   |
| NetApp SAN | NetAPP Storage Area Network, NetApp is a company<br><a href="https://www.netapp.com/us/index.aspx">https://www.netapp.com/us/index.aspx</a>   |
| NFC        | Near Field Communication  |
| NIDS       | Network Intrusion Detection System  |
| NIPP       | US National Infrastructure Protection Plan  |
| NIS        | Network and Information Security  |

|               |  |
|---------------|--|
| NIS directive | Network and Information System directive   |
| NIST          | National Institute of Standards and Technology<br><a href="https://www.nist.gov/">https://www.nist.gov/</a>  |
| NOC           | Network Operation Centre   |
| NTFS          | New Technology File System   |
| NTP           | Network Time Protocol  |
| NVRAM         | Non-Volatile Random Access Memory  |
| OASIS         | Organization for the Advancement of Structured Information Standards   |
| Oc            | Operations centre  |
| OC            | Object Controller  |
| OCC           | Operations Control Centre  |
| ODBC          | Open DataBase Connectivity   |
| OEM           | Original Equipment Manufacturer  |
| OF            | Optical Fibre  |
| ONSAFE        | Software to provide a centralized management platform remote video recording images<br><a href="https://www.lanaccess.es/soporte.php?p=descargas">https://www.lanaccess.es/soporte.php?p=descargas</a> |
| OPC-UA        | Open Platform Communications Unified Architecture  |
| OR            | Operating Room   |
| OS            | Operating System   |
| OSI           | Open Systems Interconnection   |
| OSSIM         | Open Source Security Information Management  |
| OST           | Open Storage Technology  |
| OT            | Operational Technology   |
| OTDAQ         | OT Data Acquisition  |
| PACS          | Picture Archiving and Communication System   |
| PC            | Personal Computer  |
| PCI           | Peripheral Component Interconnect  |
| PCI-DSS       | Payment Card Industry Data Security Standard   |
| PCS           | Process Control Security   |
| PCSC          | Personal Computer Smart Card   |

|          |  |
|----------|--|
| PDF      | Portable Document Format   |
| PDS      | Public Distribution System   |
| PET      | Positron Emission Tomography   |
| PIA      | Process Impact Analysis  |
| PIN      | Postal Index Number  |
| PKI      | Public Key Infrastructure  |
| PLC      | Programmable Logic Controller  |
| PoC      | Proof of Concept   |
| POC      | Point Of Contact   |
| PoE      | Power over Ethernet  |
| PPP      | Public-Private Partnership   |
| PTZ      | Pan-Tilt-Zoom, A pan-tilt-zoom camera (PTZ camera) is a camera that is capable of remote directional and zoom control.   |
| RABBITMQ | RABBIT Message Queue: It is an open source message broker software<br><a href="https://www.rabbitmq.com/">https://www.rabbitmq.com/</a>  |
| RACE     | Research and Development in Advanced Communications Technologies in Europe   |
| RADIUS   | Remote Authentication Dial-In User Service   |
| RAID     | Redundant Array of Independent Disks   |
| RAMS     | Reliability, Availability, Maintainability, and Safety as defined in EN 50126  |
| RaSTA    | Reliable and Safe Transport Application  |
| RBC      | Radio Block Centre   |
| RC2      | Rivest Cypher 2  |
| RC4      | Rivest Cypher 4<br><br>The RC4 (Rivest Cipher number 4) algorithm is a Stream encryption algorithm used for encrypting 8 bits of data that are transmitted as a continuous stream<br><a href="https://en.wikipedia.org/wiki/RC4">https://en.wikipedia.org/wiki/RC4</a> |
| RC5      | Rivest Cypher 4<br><br>Each number indicate a version of the RC algorithm, RC2 and RC5 are block symmetric key encryption algorithms again by Ron Rivest.  |
| RDBMS    | Relational Database Management System  |
| REST     | REpresentational State Transfer  |
| RF       | Radio Frequency  |

|            |  |
|------------|--|
| RFID       | Radio-Frequency Identification   |
| RGB        | Red, Green, Blue (color composition)   |
| Ril        | Richtlinie (Policy)  |
| RIPEMD-160 | RACE Integrity Evaluation Message Digest   |
| RIS        | Radiology Information System   |
| RJ45       | Registered Jack 45   |
| ROL        | Revised Operating Level  |
| RPC        | Remote Procedure Call  |
| RPMA       | Random Phase Multiple Access   |
| RPO        | Recovery Point Objective   |
| RRHH       | Human Resources Department   |
| RSA        | Rivest, Shamir and Adelman<br><br>The three inventors of this cryptographic algorithm                                |
| RSC        | Nuclear Roadmap Steering Committee   |
| RTO        | Recovery Time Objective  |
| RTU        | Remote Terminal Unit   |
| RUPAR      | Rete Unitaria della Pubblica Amministrazione del Piemonte (Unitary net of the Public Administration of the Piedmont) |
| SaaS       | Software As A Service  |
| SAN        | Storage Area Network   |
| SAP        | Systems, Applications & Products   |
| SBC        | Single Board Computer  |
| SC         | Security Control   |
| SCA        | Side Channel Analysis Attack   |
| SCADA      | Supervisory Control and Data Acquisition   |
| SCI        | Standard Communication Interface   |
| SCI-DS     | Standard Communication Interface Diagnosis   |
| SCI-ILS    | Standard Communication Interface Interlocking System   |
| SCI-LS     | Standard Communication Interface Light Signal  |
| SCI-LX     | Standard Communication Interface Railway Crossing  |
| SCI-P      | Standard Communication Interface Point   |

|         |   |
|---------|---|
| SDC     | Statistical Disclosure Control  |
| SDK     | Software Development Kit  |
| SDLC    | Secure Development Life Cycle   |
| SDR     | Software Defined Radio  |
| SDRJD   | Software Defined Radio Jammer Detector  |
| SEED    | It is a cypher algorithm<br><a href="http://seed.kisa.or.kr/html/egovframework/iwt/ds/ko/ref/%5B2%5D_SEED+128_Specification_english_M.pdf">http://seed.kisa.or.kr/html/egovframework/iwt/ds/ko/ref/%5B2%5D_SEED+128_Specification_english_M.pdf</a> |
| SEO     | Search Engine Optimisation  |
| SER2NET | Serial to Network Proxy   |
| SG      | Security Gateway  |
| SHA1    | Secure Hash Algorithm 1   |
| SHA2    | Secure Hash Algorithm 2   |
| SI      | System Information  |
| SIC     | Investment Council Secretariat  |
| SID     | System Identifier Database  |
| SIEM    | Security Information and Event Management   |
| SIFMA   | Securities Industry and Financial Markets Association   |
| SL      | Security Level  |
| SMB     | Server Message Block<br>It is a messaging protocol developed by IBM first and evolved by Microsoft  |
| SMTP    | Simple Mail Transfer Protocol   |
| SNMP    | Simple Network Management Protocol  |
| SNMPv2c | Simple Network Management Protocol v2c  |
| SNMPv3  | Simple Network Management Protocol v3   |
| SNR     | Signal to Noise Ratio   |
| SoA     | Statement of Applicability  |
| SOC     | Security Operation Center   |
| SoC     | System on-Chip  |
| SOP     | Standard Operating Procedures   |
| SQL     | Structured Query Language   |
| SRIA    | Strategic Research and Innovation Agenda  |



|           |   |
|-----------|---|
| SSH       | Secure Shell or Secure Socket Host  |
| SSL       | Secure Sockets Layer  |
| SSN       | Social Security Number  |
| ST        | Security Translator   |
| STIX      | Structured Threat Information Expression  |
| SVN       | Subversion Project Place or Repository  |
| SW        | Software  |
| TAXII     | Trusted Automated Exchange of Indicator Information   |
| TCO       | Total Cost of Ownership   |
| TCP       | Transmission Control Protocol   |
| TC-PET/CT | Positron Emission Tomography and Computed Tomography<br>Medical imaging radiological equipment  |
| TLP       | Traffic Light Protocol  |
| TLS       | Transport Layer Security  |
| TPM       | Trusted Platform Module   |
| TRL       | Technology Readiness Levels   |
| TV        | Television  |
| U2F       | Universal 2nd Factor<br><br>Open authentication standard that enables Internet users to securely access any number of online services, with one single device, instantly and with no drivers, or client software needed |
| UART      | Universal Asynchronous Receiver-Transmitter   |
| UASP      | Unitat d'Avaluació, Suport i Prevenció (Medical assistance service)   |
| UDP       | User Datagram Protocol  |
| UHF       | Ultra High Frequency  |
| UIC       | International Union of Railways<br><br><a href="https://uic.org/">https://uic.org/</a>  |
| UMTS      | Universal Mobile Telecommunications System  |
| UNB       | Ultra Narrow Band   |
| UPD       | User Datagram Protocol  |
| UPS       | Uninterruptible Power Supply  |
| URL       | Uniform Resource Locator  |

|         |   |
|---------|---|
| US      | United States   |
| USB     | Universal Serial Bus  |
| UTP     | Unshielded Twisted Pair   |
| VAR     | Value Added Reseller  |
| VDI     | Virtual Desktop Infrastructure  |
| VGA     | Video Graphics Array  |
| VHDL    | VHSIC Description Language  |
| VHSIC   | Very High Speed Integrated Circuits   |
| VLAN    | Virtual Local Area Network  |
| VLSI    | Very Large Scale Integration  |
| VM      | Virtual Machine   |
| VNC     | Virtual Network Computing   |
| VOIP    | Voice Over Internet Protocol  |
| VPN     | Virtual Private Network   |
| WAF     | Web Application Firewall  |
| WAN     | Wide Area Network   |
| WiFi    | IEEE 802.11 Wireless local area Network   |
| WLAN    | Wireless LAN  |
| WMD     | Weapon of Mass Destruction  |
| WP      | WorkPackage   |
| WPA     | WiFi Protected Access   |
| WSSC    | Water Sector Coordinating Council   |
| XFCE    | Environment desktop for various systems UniX-like   |
| XL-SIEM | Cross-Layer Security Information and Event Management   |
| XML     | Extensible Markup Language  |
| XMPP    | eXtensible Messaging and Presence Protocol  |
| XSS     | Cross-Site Scripting  |
| YAML    | YAML Ain't Markup Language<br><a href="http://yaml.org/start.html">http://yaml.org/start.html</a> |
| ZERO MQ | ZERO Message Queue  |
| ZL      | “Zuglenkung” (ZL) is a system for automatic driveway setting (Automatic Route Setting)            |

|     |   |
|-----|---|
| ZMA | Zugnummernmeldeanlage (train number system) |
|-----|---|

## Glossary updates

This glossary will have two more releases:

- The next release will be on month M30 with the new acronyms to appear in deliverables submitted on month M24: D2.5, D2.6, D3.5, D3.5, D3.7, D3.8, D3.9 and D4.1, as well as the deliverable submitted on month M27, D4.2.
- There will be a last release of this deliverable with all the acronyms and terms appeared in the CIPSEC project on month M36 at the end of the project.