ETSI GR SAI 006 V1.1.1 (2022-03)

Securing Artificial Intelligence (SAI); The role of hardware in security of AI

Disclaimer

The present document has been produced and approved by the Secure AI (SAI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/SAI-006

Keywords
artificial intelligence, cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Secure AI (SAI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document identifies the role of hardware, both specialized and general-purpose, in the security of AI. It addresses the mitigations available in hardware to prevent attacks (as identified in ETSI GR SAI 005 [i.9]) and also addresses the general requirements on hardware to support SAI (expanding from ETSI GR SAI 004 [i.8] and ETSI GR SAI 002 [i.7]). In addition, the present document reviews possible strategies for using AI for protection of hardware. The present document also provides a summary of academic and industrial experience in hardware security for AI. In addition, it addresses vulnerabilities and weaknesses introduced by hardware that can amplify attack vectors on AI.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] US NIST Glossary.

NOTE: Available at https://csrc.nist.gov/glossary.

[i.2] Recommendation ITU-T X.1252: "Baseline identity management terms and definitions".

NOTE: Available at https://www.itu.int/rec/T-REC-X.1252/en.

[i.3] Recommendation ITU-T X.1254: "Entity authentication assurance framework".

NOTE: Available at https://www.itu.int/rec/T-REC-X.1254/en.

[i.4] ISO/IEC 24760-1:2019: "IT Security and Privacy -- A framework for identity management -- Part 1: Terminology and concepts".

NOTE: Available at https://www.iso.org/standard/77582.html.

[i.5] ISO/IEC 24760-2:2015: "Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements".

NOTE: Available at https://www.iso.org/standard/57915.html.

[i.6] ISO/IEC 24760-3:2016: "Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice".

NOTE: Available at https://www.iso.org/standard/57916.html.

[i.7] ETSI GR SAI 002: "Securing Artificial Intelligence (SAI); Data Supply Chain Security".

[i.8] ETSI GR SAI 004: "Securing Artificial Intelligence (SAI); Problem Statement".

[i.9] ETSI GR SAI 005: "Securing Artificial Intelligence (SAI); Mitigation Strategy Report".

[i.10] Florian Tramèr, Dan Boneh: "Slalom: Fast, Verifiable and private execution of neural networks in trusted hardware", Proc. ICLR 2019. February 2019.

NOTE: Available at https://arxiv.org/abs/1806.03287.

[i.11] Nick Hynes, Raymond Cheng, Dawn Song: "Efficient Deep Learning on Multi-Source Private Data", July 2018.

NOTE: Available at https://arxiv.org/abs/1807.06689.

[i.12] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

NOTE: Available at https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/009/01.01.01_60/gs_nfv-sec009v010101p.pdf.

[i.13] US NIST: "Cybersecurity White Paper: Hardware-Enabled Security for Server Platforms" (draft).

NOTE: Available at https://csrc.nist.gov/News/2021/hardware-enabled-security-draft-nistir-8320.

[i.14] US NIST SP800-155: "BIOS Integrity Measurement Guidelines (draft)".

NOTE: Available at https://csrc.nist.gov/CSRC/media/Publications/sp/800-155/draft/documents/draft-SP800-155_Dec2011.pdf.

[i.15] TCG Glossary.

NOTE: Available at https://trustedcomputinggroup.org/resource/tcg-glossary/.

[i.16] GlobalPlatform GPD-SPE-009: "TEE System Architecture".

NOTE: Available at https://globalplatform.org/wp-content/uploads/2017/01/GPD_TEE_SystemArch_v1.2_PublicRelease.pdf.

[i.17] GlobalPlatform GP-REQ-025: "Root of Trust Definitions and Requirements v1.1".

NOTE: Available at https://globalplatform.wpengine.com/wp-content/uploads/2018/07/GP_RoT_Definitions_and_Requirements_v1.1_PublicRelease-2018-06-28.pdf.

[i.18] IETF RFC 8392: "CBOR Web Token (CWT)".

NOTE: Available at https://tools.ietf.org/html/rfc8392.

[i.19] IETF RFC 7519: "JSON Web Token (JWT)".

NOTE: Available at https://tools.ietf.org/html/rfc7519.

[i.20] IETF draft-ietf-rats-architecture-14: "Remote Attestation Procedures Architecture".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/.

[i.21] IETF draft-ietf-rats-eat-11: "The Entity Attestation Token (EAT)".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-rats-eat/.

[i.22] IETF draft-birkholz-rats-tuda-06: "Time-Based Uni-Directional Attestation".

NOTE: Available at https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/.

[i.23] IETF draft-ietf-rats-tpm-based-network-device-attest-11: "TPM-based Network Device Remote Integrity Verification".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/.

[i.24] IETF draft-ietf-rats-yang-tpm-charra-13: "A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/.

[i.25] IETF draft-ietf-sacm-coswid-20: "Concise Software Identification Tags".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/.

[i.26] IETF draft-ietf-sacm-epcp-01: "Endpoint Posture Collection Profile".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-sacm-epcp/.

[i.27] IETF RFC 8248: "Security Automation and Continuous Monitoring (SACM) Requirements".

NOTE: Available at https://tools.ietf.org/html/rfc8248.

[i.28] IETF RFC 8412: "Software Inventory Message and Attributes (SWIMA) for PA-TNC".

NOTE: Available at https://tools.ietf.org/html/rfc8412.

[i.29] TCG: "Runtime Integrity Preservation for Mobile Devices".

NOTE: Available at https://trustedcomputinggroup.org/resource/tcg-runtime-integrity-preservation-in-mobile-devices/.

[i.30] TCG: "Trusted Platform Module 2.0 Library".

NOTE: Available at https://trustedcomputinggroup.org/resource/tpm-library-specification/.

[i.31] TCG: "Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 / 2.0 and DICE Family 1.0".

NOTE: Available at https://trustedcomputinggroup.org/resource/tcg-tap-information-model/.

[i.32] IETF RFC 9019: "A Firmware Update Architecture for Internet of Things" (IETF Last Call).

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/.

[i.33] IETF RFC 9124: "A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-suit-information-model/.

[i.34] IETF draft-ietf-suit-manifest-16: "A Concise Binary Object Representation (CBOR)-based Serialization Format for the Software Updates for Internet of Things (SUIT) Manifest".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-suit-manifest/.

[i.35] IETF draft-ietf-teep-architecture-15: "Trusted Execution Environment Provisioning (TEEP) Architecture".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-teep-architecture/.

[i.36] MITRE: "Hardware Assurance and Weakness Collaboration and Sharing (HAWCS)" Trust & Assurance Cyber Technologies Dept., Cyber Solutions Technical Center.

NOTE: Available at https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Fall_2019/WedPM2.2_Robert_Martin.pdf.

[i.37] MITRE: data definitions.

NOTE: Available at https://cwe.mitre.org/data/definitions/1194.html.

[i.38] Overview of MITRE CWE.

NOTE: Available at https://cwe.mitre.org/about/index.html.

[i.39] Wenye Liu at al.: "Two Sides of the Same Coin: Boons and Banes of Machine Learning in Hardware Security", EEE Journal on Emerging and Selected Topics in Circuits and Systems, VOL. 11, No. 2, June 2021.

[i.40] Y.-H. Chen, et al.: "Eyeriss: An energy-efficient reconfigurable accelerator for deep convolutional neural networks" IEEE J. Solid-State Circuits, vol. 52, no. 1, pp. 127-138, January 2017.

[i.41] B. Moons and M. Verhelst: "An energy-efficient precision-scalable ConvNet processor in 40-nm CMOS", IEEE J. Solid-State Circuits, vol. 52, no. 4, April 2017.

[i.42] Y. Ma, Y. Cao, S. Vrudhula and J.-S. Seo: "Optimizing the convolution operation to accelerate deep neural networks on FPGA", IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 26, no. 7, Jul. 2018.

[i.43] S. Han et al.: "Deep compression: Compressing deep neural networks with pruning, trained quantization and Huffman coding".

NOTE: Available at http://arxiv.org/abs/1510.00149.

[i.44] S. Han et al.: "EIE: Efficient inference engine on compressed deep neural network" in Proc. ACM/IEEE 43rd Annu. Int. Symp. Comput. Archit. (ISCA), June 2016.

[i.45] P. Gysel, J. Pimentel, M. Motamedi and S. Ghiasi: "Ristretto: A framework for empirical study of resource-efficient inference in convolutional neural networks", IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 11, November 2018.

[i.46] B. Moons and M. Verhelst: "A 0.3-2.6 TOPS/W precision-scalable processor for real-time large-scale ConvNets", IEEE Symp. VLSI Circuits (VLSI-Circuits), June 2016.

[i.47] P. N. Whatmough et al.: "14.3 A 28 nm SoC with a 1.2 GHz 568 nJ/prediction sparse deep-neural-network engine with >0.1 timing error rate tolerance for IoT applications", IEEE Int. Solid-State Circuits Conf. (ISSCC), February 2017.

[i.48] DPU for Convolutional Neural Network V3.0, 2019.

[i.49] A. Tang et al.: "CLKSCREW: Exposing the perils of security-oblivious energy management", in Proc. 26th USENIX Security Symp., August 2017.

[i.50] G. Li et al.: "Understanding error propagation in deep learning neural network (DNN) accelerators and applications", Int. Conf. for High Perform. Comput., Netw., Storage, November 2017.

[i.51] A. Vakil et al.: "LASCA: Learning assisted side channel delay analysis for hardware Trojan detection", 21st Int. Symp. Qual. Electron. Design (ISQED), March 2020.

[i.52] M. Tehranipoor and F. Koushanfar: "A survey of hardware Trojan taxonomy and detection", IEEE Des. Test. Comput., vol. 27, no. 1, January 2010.

[i.53] R. Karri et al.: "Trustworthy hardware: Identifying and classifying hardware Trojans", Computer, vol. 43, no. 10, October 2010.

[i.54] M. Tehranipoor and C. Wang: "Introduction to Hardware Security and Trust", Springer, 2011.

[i.55] S. T. King et al.: "Designing and implementing malicious hardware," 1st Usenix Workshop Large-Scale Exploits Emergent Threats (LEET), 2008.

[i.56] K. Basu et al.: "CAD-base: An attack vector into the electronics supply chain", ACM Trans. Design Autom. Electron. Syst., vol. 24, no. 4, July 2019.

[i.57] C. Pilato, K. Basu, F. Regazzoni and R. Karri: "Black-hat high-level synthesis: Myth or reality?" IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 4, April 2019.

[i.58] C. Dunbar and G. Qu: "Designing trusted embedded systems from finite state machines," ACM Trans. Embedded Comput. Syst., vol. 13, December 2014.

[i.59] X. Zhang and M. Tehranipoor: "Case study: Detecting hardware Trojans in third-party digital IP cores", in Proc. IEEE Int. Symp. Hardware Oriented Security and Trust, June 2011.

[i.60] T. Iwase et al.: "Detection technique for hardware Trojans using machine learning in frequency domain", IEEE 4th Global Conf. Consum. Electron. (GCCE), October 2015.

[i.61] Y. Liu et al.: "Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs", IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 4.

[i.62] A. Kulkarni et al.: "SVM-based real-time hardware Trojan detection for many-core platform," in Proc. 17th Int. Symp. Qual. Electron. Design (ISQED), 2016.

[i.63] V. R. Carvalho and W. W. Cohen: "Single-pass online learning: Performance, voting schemes and online feature selection", in Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD), August 2006.

[i.64] Y. Jin, D. Maliuk and Y. Makris: "Post-deployment trust evaluation in wireless cryptographic ICs", in Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE, March 2012).

[i.65] J. Li, L. Ni et al.: "A novel hardware Trojan detection based on BP neural network", in Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC), Chengdu, China, October 2016.

[i.66] K. Hasegawa et al.: "Hardware Trojans classification for gate-level netlists using multi-layer neural networks", in Proc. IEEE 23rd Int. Symp. Line Test. Robust Syst. Design (IOLTS), July 2017.

[i.67] A. Kulkarni et al.: "Adaptive real-time Trojan detection framework through machine learning", in Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST), May 2016.

[i.68] K. Hasegawa et al.: "Hardware Trojans classification for gate-level netlists based on machine learning", in Proc. IEEE 22nd Int. Symp. Line Test. Robust Syst. Design (IOLTS), July 2016.

[i.69] X. Chen et al.: "A general framework for hardware Trojan detection in digital circuits by statistical learning algorithms," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 36, no. 10.

[i.70] R. Elnaggar et al.: "Run-time hardware Trojan detection using performance counters", in Proc. IEEE Int. Test Conf. (ITC), October 2017.

[i.71] H. Salmani: "COTD: Reference-free hardware Trojan detection and recovery based on controllability and observability in gate-level netlist", IEEE Trans. Inf. Forensics Security, vol. 12, no. 2.

[i.72] B. Çakır and S. Malik: "Hardware Trojan detection for gate-level ICs using signal correlation based clustering", in Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE), March 2015.

[i.73] U. Guin, D. DiMase and M. Tehranipoor: "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead", J. Electron. Test., vol. 30, no. 1, February 2014.

[i.74] US Congress: "Ike Skelton national defense authorization act for fiscal year 2011", U.S. Government Printing Office, Tech. Rep., 2011.

[i.75] K. Mahmoodet et al.: "Real-time automated counterfeit integrated circuit detection using X-ray microscopy", Appl. Opt., vol. 54, no. 13, 2015.

[i.76] N. Asadizanjani et al.: "Counterfeit electronics detection using image processing and machine learning", J. Phys., Conf. Ser., vol. 787.

[i.77] A. Ahmadi et al.: "A machine learning approach to fab-of-origin attestation", Proc. 35th Int. Conf. Comput.-Aided Design, November 2016.

[i.78] B. Ahmadi et al.: "Automated detection of counterfeit ICs using machine learning", Microelectron. Rel., vols. 88-90, September 2018.

[i.79] X. Zhang et al.: "Path-delay fingerprinting for identification of recovered ICs", Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT), October 2012.

[i.80] M. M. Alam et al.: "Recycled FPGA detection using exhaustive LUT path delay characterization", Proc. IEEE Int. Test Conf. (ITC), November 2016.

[i.81] A. Stern et al.: "EMFORCED: EM-based fingerprinting framework for counterfeit detection with demonstration on remarked and cloned ICs", Proc. IEEE Int. Test Conf. (ITC), October 2018.

[i.82] K. Huang et al.: "Parametric counterfeit IC detection via support vector machines", Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT), October 2012.

[i.83] H. Dogan et al.: "Aging analysis for recycled FPGA detection", Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT), October 2014.

[i.84] K. Huanget al.: "Recycled IC detection based on statistical methods", IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 34, no. 6, June 2015.

[i.86] S. Sharma and K. Chen: "Confidential machine learning on untrusted platforms: a survey", Cybersecurity 4, 30 (2021).

NOTE: Available at https://doi.org/10.1186/s42400-021-00092-8.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

attack surface: total number of attack vectors that an attacker can use to manipulate a network or computer system or extract data

attack vector: method or way an attacker can gain unauthorized access to a network or computer system

authentication: verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

NOTE: From US NIST Glossary [i.1].

authorization: access privileges granted to a user, program, or process or the act of granting those privileges

NOTE: From US NIST Glossary [i.1].

availability: ensuring timely and reliable access to and use of information

NOTE: From US NIST Glossary [i.1].

Client Application (CA): application running outside of the Trusted Execution Environment making use of the TEE Client API to access facilities provided by Trusted Applications inside the Trusted Execution Environment

NOTE: From Global Platform GPD-SPE-009 [i.16].

confidentiality: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

NOTE: From US NIST Glossary [i.1].

context: environment with defined boundary conditions in which entities exist and interact

NOTE: From Recommendation ITU-T X.1252 [i.2].

cybersecurity: prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

NOTE: From US NIST Glossary [i.1].

entity: something that has separate and distinct existence and that can be identified in a context

NOTE: From Recommendation ITU-T X.1252 [i.2].

Entity Authentication Assurance (EAA): degree of confidence reached in the authentication process that the entity is what it is, or is expected to be

NOTE 1: This definition is based on the 'authentication assurance' definition given in Recommendation ITU-T X.1252 [i.2].

NOTE 2: The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented. Recommendation ITU-T X.1254 [i.3].

firmware image: binary that can contain the complete software of a device or a subset of it

NOTE 1: The firmware image can consist of multiple images, if the device contains more than one microcontroller. Often it is also a compressed archive that contains code, configuration data, and even the entire file system. The image can consist of a differential update for performance reasons.

NOTE 2: From IETF RFC 9019 [i.32].

Hardware-Mediated Execution Enclave (HMEE): area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave and which is protected from eavesdropping, replay, and alteration attacks as the programs within the enclave are executed

NOTE: Derived from ETSI GS NFV-SEC 009 [i.12].

identity: set of attributes related to an entity

NOTE: Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context. (from ISO/IEC 24760 [i.4] to [i.6]).

integrity: property that data or information have not been altered or destroyed in an unauthorized manner

NOTE: From US NIST Glossary [i.1].

manifest: meta-data about the firmware image which is protected against modification and provides information about the author

NOTE: Derived from IETF RFC 9019 [i.32].

mutual authentication: authentication of identities of entities which provides both entities with assurance of each other's identity

NOTE: Derived from Recommendation ITU-T X.1254 [i.3].

non-repudiation: ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action

NOTE: Derived from Recommendation ITU-T X.1252 [i.2].

platform: any computing device (regardless of its architecture or operating system)

platform integrity: verifiable state of complete assurance that, under all conditions, a computing system has a correct and reliable operating system, logically complete hardware, firmware, and software, and system isolation and protection mechanisms (e.g. memory access control, process isolation, data integrity, etc.)

Relying Party (RP): actor that relies on an identity assertion or claim

NOTE: Derived from Recommendation ITU-T X.1254 [i.3].

Rich Execution Environment (REE): execution environment comprising at least one device OS or Rich OS and all other components of the device (SoCs, other discrete components, firmware, and software) which execute, host, and support the Rich OS (excluding any TEEs and SEs included in the device)

NOTE: WARNING: In a previous version of Global Platform GPD-SPE-009 [i.16] the REE was considered to be everything outside of the TEE under consideration. In the new definition other entities are acknowledged. Contrast *Trusted Execution Environment*. Global Platform GPD-SPE-009 [i.16].