

DISCLAIMER

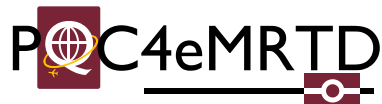
This document, D3.2 – Report on the Standardization work on PQC, HPC and quantum computing hardware and software, has been prepared as part of the PQC4eMRTD project, under Grant Agreement No 101190400, and is currently under review by the European Commission. It is provided for informational purposes only.



Funded by
the European Union



ECCE 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE





D3.2 – Standardization work on PQC, HPC and quantum computing hardware and software

Project number: 101190400

Project name: Post-Quantum Cryptography for electronic Machine-Readable Travel Documents

Project acronym: PQC4eMRTD

Document Information:	
Work Package No:	3
Lead Beneficiary:	BSC
Type:	Report
Dissemination Level:	Public
Written by:	Leonidas Kosmidis (BSC), Matina Maria Trompouki (BSC)
Approved by:	Antonio Escobar (IFAG)
Reviewed by:	Detlef Houdeau (IFAG)
Version:	v1.0
Submission Date:	30/09/2026
Due Date:	30/09/2026



**Funded by
the European Union**



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

PQC4eMRTD has received funding from the European Union's Digital Europe Programme (DIGITAL) under Grant Agreement No 101190400 and is supported by the European Cybersecurity Competence Centre.

Document Control Page:

Version	Date	Author(s)	Changes
v0.1	14/08/2026	Leonidas Kosmidis, Matina Maria Trompouki	First draft
v0.2	21/08/2026	Matina Maria Trompouki	References added
v0.3	15/09/2026	Leonidas Kosmidis, Matina Maria Trompouki	Final deliverable before review
v0.4	18/09/2026	Matina Maria Trompouki	Reviewed version
v0.5	22/09/2026	Matina Maria Trompouki	Reviewed version
v0.6	25/09/2026	Matina Maria Trompouki	Revised after review
v0.9	30/09/2026	Leonidas Kosmidis	Version released for internal review
v1.0	30/09/2026	Antonio Escobar	Detlef Houdeau comments implemented; front matter, acronyms and spelling harmonised with the project template; approval gate by IFAG; released for submission

The PQC4eMRTD Consortium

#	Partner Legal Name	Short Name	Role	Country
1	INFINEON TECHNOLOGIES AG	IFAG	Coordinator	Germany
2	THALES CDI FRANCE SAS	THALES CDI	Beneficiary	France
3	INSTITUT ZA PRIMERJALNO PRAVO PRI PRAVNI FAKULTETI V LJUBLJANI	IPP PFLJUBLJANA	Beneficiary	Slovenia
4	BARCELONA SUPERCOMPUTING CENTER CENTRO NACIONAL DE SUPERCOMPUTACION	BSC	Beneficiary	Spain
5	CRYPTONEXT SECURITY	CRYPTONEXT	Beneficiary	France



Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. This material is the copyright of PQC4eMRTD consortium parties, and may not be reproduced or copied without permission. The commercial use of any information contained in this document may require a licence from the proprietor of that information.

Table of Contents

1. Introduction	8
2. Contributions to RISC-V Standardisation	9
2.1 RISC-V Participation and Ratification Procedures	9
2.2 Participation to the RISC-V Security Groups	11
2.3 Participation, Monitoring and Updates of relevant RISC-V Groups.....	13
2.4 Contributions to Software Implementations and Linux Foundation Projects	16
3. Participation, Monitoring and Updates for PQC in Other Domains	18
2.5 Participation and Updates in Horizontal Standards and Industrial Automation.....	18
2.6 Updates in Automotive.....	19
2.7 Participation and Updates in Avionics	19
2.8 Participation and Updates in Space	20
4. Conclusion.....	22
References	23

List of Tables

Table 1 RVM Profile Ratification Plan as of September 2026 15

Acronyms

ACE	Atomic Cryptography Extension
ADHA	Advanced Data Handling Architecture
AIT	Assembly, Integration, and Test
API	Application Programming Interface
ARC	Architecture Review Committee
AUTOSAR	Automotive Open System Architecture
BLAS	Basic Linear Algebra Subprograms
BoD	Board of Directors
BSC	Barcelona Supercomputing Center
CCSDS	Consultative Committee for Space Data Systems
CPU	Central Processing Unit
DASC	Digital Avionics Systems Conference
EASA	European Union Aviation Safety Agency
ECSS	European Cooperation for Space Standardization
ELISA	Enabling Linux in Safety Applications
EMC	Electromagnetic Compatibility
eMRTDs	electronic machine-readable travel documents
ESA	European Space Agency
ESTEC	European Space Research and Technology Centre
EU	European Union
FALCON	Fast Fourier lattice-based compact signatures over NTRU
FFT	fast-Fourier transform
FIPS	Federal Information Processing Standard
FN-DSA	Fast-Fourier transform over NTRU-Lattice-Based Digital Signature Algorithm
FPGA	Field-Programmable Gate Array
GPU	Graphics Processing Unit
HAC	High Assurance Cryptography
HADES	Hardware Dependability for Embedded Systems
HQC	Hamming Quasi-Cyclic
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standardization
METASAT	Modular Model-based Design and Testing for Applications in Satellites
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MQOM	MQ on my Mind
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OpenGL	Open Graphics Library
PAS	Publicly Available Specification
PQC	Post-Quantum Cryptography
QEMU	Quick Emulator
QR-UOV	Quotient Ring Unbalanced Oil and Vinegar

RISC-V	Reduced Instruction Set Computer Five
RTEMS	Real-Time Executive for Multiprocessor Systems
RTOS	Real-Time Operating System
RVA23	RISC-V Application Profile 2023
RVM	RISC-V Microcontroller
SAE	Society of Automotive Engineers
SafeComp	International Conference on Computer Safety, Reliability, and Security
SAVOIR	Space AVionics Open Interface aRchitecture
SBDC	Space-Based Data Centres
SC	Safety Critical
SDitH	Syndrome-Decoding-in-the-Head
SHA-3	Secure Hash Algorithm 3
SIGs	Special Interest Groups
SIMD	Single Instruction, Multiple Data
SMARTY	Scalable and Quantum Resilient Heterogeneous Edge Computing enabling Trustworthy AI
SMC-IT	International Conference on Space Mission Challenges for Information Technology
SQLsign	Short Quaternion and Isogeny Signature
TGs	Task Groups
TSC	Technical Steering Committee
UOV	Unbalanced Oil and Vinegar
WP	Work Package

1. Introduction

In the deliverable D2.2 [1] RISC-V has been identified as the major standardisation body in which the project could participate, due to its proliferation to all types of systems, spanning from supercomputers, to Internet of Things (IoT) devices like the chips found in electronic machine-readable travel documents (eMRTDs). In addition, the participation of project members in RISC-V committees and holding key positions in them has been a decisive factor for this selection. Moreover, the existence of task groups and special interest groups in embedded, real-time and safety critical systems which have similar requirements with eMRTDs offered several opportunities to benefit from existing standardised solutions from other domains, instead of replicating efforts which might result in fragmentation and may hinder Post-Quantum Cryptography (PQC) migration.

In this deliverable, we provide details about the project's contributions to standardisation, mainly in RISC-V as well as in the other identified bodies.

2. Contributions to RISC-V Standardisation

In the deliverable D2.2 [1] several relevant RISC-V Special Interest Groups (SIGs) and Task Groups (TGs) have been identified and were monitored during the project. In particular, the deliverable D2.2 [1] contained the monitoring of these groups until April 2025, which was the delivery date. In this deliverable, we include both the contributions of the project to these groups, as well as the updates on the most important TGs and SIGs that are related to the EU Cyber Resilience Act (CRA; EU 2024/2847), which has been the cornerstone of the PQC migration.

PQC4eMRTD partners namely Barcelona Supercomputing Center (BSC) and Infineon have been RISC-V members before the project started. However, given the need of active participation in RISC-V standardisation committees in order to influence the standardisation regarding the adoption and use of PQC not only in high-performance devices (i.e. high-performance computers, supercomputers, desktop computers etc), but also in resource-constrained systems, all the necessary actions to do so have been taken.

This included first understanding the formal procedures that RISC-V International has in place in order to allow such participation. After complying with them, regular participation in the weekly meetings has been performed, together with participation in the face-to-face events in Europe and America, and participation in all voting procedures. In the next subsections, we provide more information about these.

2.1 RISC-V Participation and Ratification Procedures

RISC-V International has been accepted by the International Organization for Standardization (ISO) as an ISO/PAS (Publicly Available Specification) submitter in 2025. Moreover, during 2025 an important reform has been applied to its governance, imposing new stricter procedures that need to be followed by each SIG and TG.

Participation to RISC-V meetings is only permitted to members of RISC-V International. RISC-V maintains mailing lists for each of its SIGs and TGs, whose archives are publicly available [2]. The archive of some mailing lists however is only accessible by members of those particular lists.

In order to register to a mailing list, an account needs to be created, and request access to that list. After the membership status of the account is verified by RISC-V International, inscription to the mailing list is performed. Joining a mailing list does not provide membership to a SIG or TG and therefore voting rights. However, only mailing list subscribers are able to post to that list.

RISC-V International maintains a collection of Jira spaces [3] which hold the related information of each SIG and TG. Each SIG and TG publishes their Charter, Participation status and voting rights, minutes of their weekly meetings and other relevant documents produced by them, including white papers and others.

Each SIG and TG meets weekly, however few of them choose to meet biweekly or monthly. Twice per year, elections take place in each SIG and TG for the Chair and Vice Chair positions. Election announcements are sent to the mailing lists, asking for nominations, and any RISC-V member is eligible to nominate themselves for the Chair or Vice-Chair positions. The candidate needs to provide a short statement about their plans for the position they are volunteering for and a short biographic statement. Candidates do not get voting rights automatically.

In order to obtain voting rights to newly created SIGs and TGs, one needs to include their name in the Participation Status and Voting rights Jira page before the start of the election period. Only one member from a given organisation can have voting rights, while the rest can only have participant and observer roles. RISC-V International after verifying the membership of the account and the aforementioned requirement, can approve the voting, or membership status with respect to the particular SIG and TG. For existing SIGs and TGs, participation rights are obtained by attending regularly the meetings of the corresponding SIG and TG and expressing their interest to become a voting member or participant to the Chair. The chair needs to record this in the meeting minutes and the Participation status and Voting register, and then the candidate voting member enters a probation status for the next 3 meetings. Once the member has attended the following 3 consecutive meetings of the SIG or TG, they can exit the probation status and obtain full voting status.

However, in order to maintain their voting status, a member must attend 2 out of the 3 last meetings, as well as exercise their voting right in all TG or SIG elections. This includes elections for the Chair and Vice-Chair, Development Milestones and Specification Ratification. In-person meetings in the RISC-V Summit North America and RISC-V Europe which take place on the members' day contribute to the attendance too.

Therefore, in order to contribute to RISC-V standardisation, consistent attendance and participation is required. In addition, considering the number of standardisation groups that are addressed in the project, the effort required from the project members has been considerable.

In summary, BSC has participated as a voting member via Dr. Leonidas Kosmidis in the Post Quantum Cryptography TG, the High Assurance Cryptography (HAC), the Crypto SIG and the Space SIG. Moreover, Dr. Leonidas Kosmidis has been candidate for the Vice Chair positions in the Packed Extension TG, Space SIG and RISC-V Microcontroller (RVM) Profile TG, and has been elected as Vice Chair in the RVM profile. He has also been a founding member of the Space SIG, and has been attending less frequently the Functional Safety SIG, Automotive SIG, Vector SIG, and Packed Single Instruction, Multiple Data (SIMD) TG.

Infineon has been participating indirectly in the RVM Profile standardisation through their joint venture Quintauris, which chairs the RVM profile TG, and directly in the Automotive and Functional Safety SIGs.

Throughout this period, the HAC Specification is close to ratification with its Development Milestone Approved, as well as the PQC TG with its Internal Review completion. Moreover, the RVM TG had its Ratification Plan approved and held several Architecture Review Committee (ARC) meetings to receive feedback. The Space SIG has authored two white papers, one survey on RISC-V for Space, as well as a space datacenters whitepaper. Finally, the Functional Safety SIG published a white paper and the Packed extension has reached its Development Milestone. The following subsections provide detailed information about these standardisation efforts.

2.2 Participation to the RISC-V Security Groups

BSC has been a voting member in the Crypto SIG, the PQC TG and HAC TG, contributing to their specifications with the requirements stemming from the PQC4eMRTD project, mainly from the IoT domain, as well as safety critical domains.

Post Quantum Cryptography Task Group (PQC TG)

Until BSC's involvement in the groups, the PQC TG considered only the case of PQC acceleration using vector instructions. However, vector instructions are only available in high-end Central Processing Units (CPUs), targeting the server, desktop and high-performance domains. The project raised awareness about this issue through its first attendance at RISC-V Summit North America 2025, with a presentation on the members' day [4] and a poster presentation in the Summit program, in the Security Posters Session [5]. Subsequent information and feedback were provided during the weekly meetings and discussions regarding the ongoing research at BSC in resource-constrained alternatives through custom instructions and the use of packed instructions which are significantly less resource-demanding for IoT devices. An additional poster was presented in RISC-V Summit Europe 2026 [6].

As of September 2026, the PQC TG has completed its Internal Review about a Vector Keccak permutation extension which is used by the National Institute of Standards and Technology (NIST) Secure Hash Algorithm 3 (SHA-3) and several PQC algorithms. The extension comes with a prototype RISC-V core implemented on an FPGA, Karu64, as well as a QEMU implementation and reference code implementation.

The packed extension PQC acceleration methods which are currently implemented in BSC will be included in a subsequent release after they mature and are published in a scientific publication.

High Assurance Cryptography Task Group (HAC TG)

Unlike PQC TG, the HAC TG had already considered a generic specification without assuming special features for the implementation of the high assurance cryptographic primitives of its specification. This makes the specification applicable also to IoT constrained devices as it is the case of eMRTDs. The HAC specification, originally called ACE but recently (September 2026)

renamed KLEE, defines a multitude of cryptographic algorithms that can be used through its secure interface. PQC algorithms are included in the list of the predefined cryptographic algorithms. Therefore, our participation was mainly to ensure that both the resource constraints of the PQC4eMRTD project domain requirements and the inclusion of PQC algorithms were included in the specification. The HAC TG passed its internal review in August 2026, and proceeded with the Development Milestone approval in September 2026.

Crypto SIG

The Crypto SIG oversees the Post Quantum Cryptography (PQC) and High Assurance Cryptography (HAC) TGs and their milestones. During the meetings, common topics related to monitoring PQC and Cryptography state of the art developments and standardisation were discussed. The most important developments discussed were the following:

- NIST is currently working on a draft for the standardisation of HQC (Hamming Quasi-Cyclic) algorithm, which will serve as back-up algorithm for ML-KEM. HQC is based on a different mathematical problem, which provides confidence that if a weakness is discovered in ML-KEM, an alternative will be in place. The finalised standard is expected in 2027. See also the deliverable D3.3.
- NIST is also working on a draft for the standardisation of FALCON, which is a lattice-based digital signature scheme. Unlike the rest of cryptographic algorithms, FALCON relies on floating-point arithmetic, which increases hardware requirements in terms of supported features. However, FALCON reduces the size of the keys and signatures which are required compared to ML-DSA, which is particularly important for eMRTD use cases. FALCON is in draft status and is expected to be published in 2027, as FIPS 206 FN-DSA (FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm).
- Nine PQC candidate algorithms have advanced to the third round of the Additional Digital Signatures process and are considered by NIST for standardisation: FAEST, HAWK, MAYO, MQOM, QR-UOV, SDitH, SNOVA, SQIsign, UOV [7].
- On 28 July 2026, Anthropic announced that it had used an AI model to discover a vulnerability in the lattice-based digital signature algorithm HAWK, which was among the candidates for standardisation. Following the announcement, the HAWK development team withdrew the algorithm from NIST consideration [7].
- Similar to NIST, China has ongoing competitions for the development and standardisation of their PQC algorithms.

2.3 Participation, Monitoring and Updates of relevant RISC-V Groups

The previous section included the most relevant activities to the PQC4eMRTD project, which were directly related to PQC standardisation. However, as discussed in D2.2 [1], there are also highly related RISC-V TGs and SIGs which have similar requirements with eMRTDs, IoT and embedded systems.

Packed SIMD Extension TG

The Packed SIMD Extension is viewed by BSC as the most cost-effective solution to accelerate PQC algorithms, and BSC is currently working towards this. As a consequence, the work of the Packed SIMD extension TG is highly relevant. The Packed extension remained in draft status for a long time and its development had paused, but it was revived in 2025.

The specification has been overhauled, with new instruction naming for consistency with the vector specification, the introduction of floating-point packed instructions and compiler support for datatypes and intrinsics. As of September 2026, the Packed SIMD is under voting to complete its Development Milestone.

Space SIG

The space domain has been identified as one of the most relevant domains to eMRTDs, because the two share common requirements such as long lifetimes (20 years) and both are resource-constrained in terms of area and power consumption. The Space SIG was established in 2025, had its Charter approved and had its first meeting at RISC-V Summit North America 2025. BSC has been among the founding members of the SIG, and Dr. Leonidas Kosmidis was a candidate for the Vice Chair position. The working group started its biweekly meetings in early 2025 and had an in-person meeting at RISC-V Summit Europe 2026 during the members' day, where it organised a very well attended event. The event was a half-day thematic session RISC-V in Space, with presentations from key stakeholders in the space industry as well as an open discussion.

During the members' day at RISC-V Summit Europe 2026, two joint meetings were organised, one with the PQC TG in which Dr. Leonidas Kosmidis represented BSC in both TGs/SIGs as well as another meeting with the HPC SIG. The former focused on the emerging security requirements that need to be taken into consideration in space, while the latter focused on the synergies between HPC and the space, which requires increasing levels of performance and lately includes data centres in space.

The Space SIG has authored a document about the state of the art of RISC-V in space and what is needed for the transition of the space domain to RISC-V [8]. The first version of the document was released before the thematic session at RISC-V Summit Europe 2026, in order to receive

further feedback. The Space SIG is currently working on addressing the received comments and on releasing a new version soon.

In addition, the Space SIG has worked on a document about Orbital Data Centers [9]. In this document, the Space SIG advocates about why RISC-V is a good candidate for this new concept of operations. The purpose of the early version of the document is to receive feedback before European Space Agency's (ESA) Strategic Initiative on Space-Based Data Centres (SBDC) event which is being organised in November 2026 at European Space Research and Technology Centre (ESTEC). After the event, the document will be updated based on the comments that will be received.

RVM Profile TG

Microcontrollers have very similar requirements with eMRTDs, since they are the processing technology used in them. Therefore, their specification is very relevant to the project. The RVM Profile TG focuses on the definition of a common set of RISC-V extensions that will need to be implemented by RISC-V microcontrollers which will be compliant with this profile.

The main reason behind the development of the profile is to reduce fragmentation of the software ecosystem. A similar work has been already completed with the RVA23 profile which was ratified in October 2024. This profile that targeted the RISC-V application cores, defined the set of RISC-V extensions that need to be supported by the compliant architectures. This enables the Linux Kernel, Linux distributions and toolchain providers, to provide a single release of their products which can target the compliant devices. Still the implementers can have the flexibility to support other RISC-V extensions, which is the benefit of RISC-V's instruction set, but in this case, they (or their users) will need to compile the toolchains, the Linux Kernel and the software of the distributions themselves. The concept is exactly the same in the RVM profile, but targeting real-time operating system providers and toolchain providers.

The RVM profile preexisted since 2024-2025 and its creation was backed by both Infineon and its joint venture QuinTauris. However, it stopped operations in 2025 due to the unavailability of the TG leadership. In December 2025 a new election was announced, with QuinTauris and BSC leading the TG, with an aggressive plan to achieve ratification by end of 2026 or early 2027. The TG has been meeting biweekly and got its Ratification Plan approved by TSC (Technical Steering Committee).

The TG met in person at RISC-V Summit Europe 2026 on the members' day, where it presented the plan for the two work packages (WP) that will be included in the proposed profile. WP1 focuses on low-end microcontrollers while WP2 focuses on high end ones.

An initial proposal of the extensions to be included was made and provided to the mailing list and TG participants in the form of survey, in order to indicate their preference on the features that need to be included. Moreover, invited presentations by Real Time Operating System (RTOS)

providers and toolchain vendors have been planned for September to November 2026, in order to provide their feedback.

The profile will offer compatibility among different microcontrollers in terms of features/extensions, but not binary compatibility as RVA. The reason is that RTOSes are usually distributed as source code/precompiled object files and libraries, but the final executable is generated and includes the user code, since both share the same address space. Moreover, microcontrollers do not include a memory management unit and may have significantly different memory map.

Milestone	Date
Plan Approval	Oct 7, 2026
Internal Review Start	Nov 4, 2026
Specification Stabilized	Dec 16, 2026
ARC Review Freeze Request	Jan 13, 2027
Freeze	Feb 3, 2027
Public Review Start	Mar 3, 2027
TSC Ratification Approval	May 9, 2027
BoD Ratification Approval	May 27, 2027

Table 1 RVM Profile Ratification Plan as of September 2026

Table 1 shows the current ratification plan of the profile as of September 2026. Despite the final ratification planned for Q2 2027, the profile will be stable by end of 2026.

The naming of the Profile is not finalised yet, but it is an issue that has been deliberated significantly, and it is up to the board to select.

Functional Safety SIG

The Functional Safety SIG has been one of the oldest SIGs/TGs which are relevant to the PQC4eMRTD related works, since these systems primarily rely on microcontrollers. BSC held a leadership position in the SIG until 2024, and kept participating in the biweekly meetings together with Infineon.

The Functional Safety SIG met in person at RISC-V Summit Europe 2025 during the members' day, with the BSC participation and announced the availability of their first version of the RISC-V Functional Safety white paper. A revised version of the document became available in December 2025 [10]. An additional in-person meeting took place at RISC-V Summit Europe 2026 during the members' day, too.

The SIG featured invited speakers from the real-time, embedded and safety critical systems domain to present their state-of-the-art research on topics related to the TG. This includes performance monitoring and quota enforcement solutions which are required both for functional safety and security. BSC has presented in one of the meetings their Safe SU (statistic unit) which provides such functionality.

Automotive SIG

After Functional Safety, the Automotive SIG is the next most relevant to PQC4eMRTD, because it is closely tied to the Functional Safety and microcontrollers, which are typically used in these systems. The Automotive SIG meets biweekly and follows a similar approach with the RVM and Functional Safety, with surveys in which members provide feedback as well as invited speakers.

The Automotive SIG has produced a white paper which is currently in draft form. The document includes chapters on security, virtualisation and auto-coding tools, debug and tracing. The former two are of significant interest for PQC4eMRTD, since post-quantum resilience is included. Moreover, the use of virtualisation can help to provide both safety and security in the platform.

Soft CPU SIG

The soft CPU SIG focuses on the implementation of CPUs in reconfigurable architectures like FPGAs, in which the processors can be configurable and customised. It oversees the Composable Custom Extensions TG, which focused on the addition of custom extensions in these soft cores, and an easy way to add compiler support for them.

The Soft CPU SIG had an in-person meeting at RISC-V Summit Europe 2026 during the members' day, in which BSC participated. BSC conducts research on alternative, low-cost ways to accelerate PQC algorithms, as the ones presented in [5], some which include custom instructions. Even though eMRTDs are not expected to use FPGAs, FPGAs offer a research platform to experiment with these solutions. Custom instructions that can be prototyped and demonstrated in this way can be later implemented in ASICs and obtain the same benefit.

2.4 Contributions to Software Implementations and Linux Foundation Projects

Deliverable D2.2 [1] mentioned liboqs, from the Open Quantum Safe (OQS) project, of the Linux Foundation's Post-Quantum Cryptography Alliance project, which provides reference algorithm implementations. Moreover, it mentioned that Graphics Processing Unit (GPU) accelerated software implementations of PQC algorithms have been released by NVIDIA as part of the cuPQC library. NVIDIA released the version 0.4 of the library in September 2025, including additional features like additional hashing algorithms and Merkle trees. However, similar to most of

NVIDIA's libraries, such as cuBLAS, cuFFT, cuDNN and cuSparse, cuPQC is a closed-source library which can only benefit NVIDIA GPUs. Recently, an open source CUDA implementation of ML-KEM was released, ICICLE, by Ingonyama [11].

Dr. Leonidas Kosmidis participates in several Khronos committees, especially for safety critical systems. In particular, he is the Chair and Outreach officer of the SYCL SC (Safety Critical) Working Group, in which he advocates about the use of open standards in GPU programming. Moreover, he is participating in the Vulkan SC Advisory Forum, OpenGL SC and OpenCL working groups. As part of his involvement in Khronos, which is also supported by the PQC4eMRTD, he has co-led the working group development of the SYCL SC specification which is still under development.

Moreover, at BSC he supervises on-going work for the acceleration of PQC algorithms in GPUs, using open standards such as OpenCL, OpenGL SC 2.0, Vulkan (SC) and SYCL. This work is still under development and will be released as open source when it is completed and published. The work uses the same interface as cuPQC, providing a drop-in replacement for the library. In that regard, it uses cuPQC as a standardised Application Programming Interface (API) similar to what other widely used libraries do with their variants such as Basic Linear Algebra Subprograms (BLAS), FFTW etc.

Additional work at BSC addresses the development of GPU implementations for Homomorphic Encryption. Homomorphic Encryption uses the same building block as PQC algorithms, the Number Theoretic Transform (NTT).

In addition to the aforementioned Linux Foundation projects, BSC has participated in other Linux Foundation projects, namely ELISA (Enabling Linux in Safety Applications). ELISA has several working groups, however the most relevant ones for PQC4eMRTD are the Aerospace Working Group and the Space Grade Linux WG, as well as the Aerospace Use Case WG. Dr. Leonidas Kosmidis supported by PQC4eMRTD has actively participated in these Working Groups, in the online weekly meetings as well as in the in-person/hybrid meetings of the Foundation, in Munich during November 2025.

During this time, the aerospace working group has started authoring a scientific paper in the form of a survey, whose abstract was submitted to the Digital Avionics Systems Conference (DASC) 2026, and was accepted. However, the final paper was not completed in time and therefore it was not finally submitted. The document is still under development due to the large body of literature that it covers. In the initial draft the paper was covering both avionics and space systems, however the WG decided to split them in two separate papers. Other work in the aerospace working group is to collect requirements from other similar efforts from safety critical domains. Dr. Leonidas Kosmidis participated in providing information about space systems and qualification effort undergoing at ESA regarding Real-Time Executive for Multiprocessor Systems (RTEMS) as well as from research projects at BSC in the automotive domain, and in the particular

case of virtualisation. Moreover, the WG prepared a presentation about Virtualisation which has been delivered as a webinar in the wider ELISA community.

In Space Grade Linux, invited presentations from relevant stakeholders were given in its meetings, including solutions to deal with the reliability of file systems in space, fault injection and hypervisor technologies, which are also a common theme with the technologies used in other critical systems and covered in the previous section about RISC-V WGs. Currently Space Grade Linux is transitioning to an independent Linux project, which will be launched in Q1 2027. BSC has applied to become a founding associate member since September 2026.

The Aerospace Use Case WG is a technical WG which develops an aerospace use case that can be used to demonstrate the use of Linux in such a context. The WG has prepared a minimal tutorial on how to setup the use case, accompanied by a video tutorial which has been released in the wider ELISA community.

BSC has been officially accepted as an associate member of the ELISA project in September 2026.

3. Participation, Monitoring and Updates for PQC in Other Domains

The deliverable D2.2 identified additional domains and standardisation relevant to PQC4eMRTD in which the project members can participate and influence. Several of those have been covered in the previous section because they were related to RISC-V and Linux Foundation projects. In this section we provide the remaining ones.

2.5 Participation and Updates in Horizontal Standards and Industrial Automation

The previously identified CENELEC (European Committee for Electrotechnical Standardization), CEN and ETSI European Standardisation Organisations for Horizontal Standards have not yet produced any openly accessible outcome that the consortium members are aware of. The same applies to ISA/IEC 62443 “Security for industrial automation and control systems” series of standards for industrial automation. Moreover, due to the limited manpower and available effort, as well as the difficulty to be admitted to participate in these standardisation organisations, the consortium did not participate in them.

Subcommittees and Working Groups (running under Cyber Resilience Act)

CLC/TC 47X/WG 01 Microprocessors and Microcontrollers with security related functionalities; the work is focused on defining harmonised standards enabling self-assessment of Cyber Resilience Act (CRA)

CLC/TC 47X/WG 02 Tamper resistant Microprocessors and Microcontrollers; this is focused on developing harmonised European standards to support compliance with the EU [Cyber Resilience Act](#)

CLC/TC 47X/WG 03 Smart Cards and Secure Element Platforms; Harmonising Common Criteria Protection Profiles and developing standards such as EN 50764, which addresses the cyber resilience of EUCC (EU Common Criteria) certified platforms for smartcards and similar secure element devices.

2.6 Updates in Automotive

The main part of Automotive standardisation was covered in the previous section in relation to the Automotive and Functional Safety SIGs in RISC-V International. Regarding the Automotive Cybersecurity standards, no new updates have been issued for “ISO/SAE 21434 Road vehicles — Cybersecurity engineering” nor in the “UNECE WP.29 automotive cybersecurity” standards. Similarly, no new updates have been released by Automotive Open System Architecture (AUTOSAR) in relation to cyber security and post-quantum cryptography. It is worth noting that AUTOSAR has an established connection with Khronos Safety Critical working groups, and therefore related updates can reach AUTOSAR, too.

2.7 Participation and Updates in Avionics

As with Automotive, the updates related to Avionics have been covered in the previous section, mainly through the participation in the aerospace working groups of ELISA. Despite that, no updates have been released for DO-326A / ED-202A “Airworthiness Security Process Specification” [12] nor for DO-355 / ED-204A - Information Security Guidance for Continuing Airworthiness [13].

Although the consortium members are not participating in the European Union Aviation Safety Agency (EASA) and Society of Automotive Engineers (SAE) working groups that develop and maintain the aforementioned standards, Dr. Leonidas Kosmidis has a constant presence in the most important avionics conference, in which members of these working groups participate, and has the potential to influence their directions.

In both editions of 2025 and 2026 of the Digital Avionics Systems Conference (DASC), Dr. Leonidas Kosmidis taught two tutorials, one about Certifiable GPU programming for Safety Critical Systems and one about Introduction to RTEMS, the real-time operating system supported in the Modular Model-based Design and Testing for Applications in Satellites (METASAT) platform [14]. The first tutorial was focused on the programming of GPUs using Khronos’ open APIs, including OpenGL SC 2.0, Vulkan SC and SYCL (SC) which are used in BSC for the implementation of GPU accelerated PQC algorithms as mentioned in section 2.4. Moreover, the second tutorial included information about how to develop an RTEMS driver for the Vortex GPU which is included in the METASAT FPGA platform, developed in the METASAT EU funded project, and it is currently used for the development of PQC GPU acceleration algorithms.

2.8 Participation and Updates in Space

As in the previous safety critical domains, the related activities have been mainly covered in the previous section, through the participation in the Space SIG of RISC-V as well as in the Aerospace and Space Grade Linux WGs of ELISA.

In addition to them, although BSC does not directly participate in Consultative Committee for Space Data Systems (CCSDS), as its members are space agencies and aerospace industrial entities, it does indirectly influence CCSDS standardisation through dissemination of the PQC4eMRTD project and the PQC related research conducted at BSC, through participation in key events and scientific publications in relevant events.

Dr. Leonidas Kosmidis participated in the Flight Software Workshop 2026, in which he delivered a presentation on the application of PQC in space systems [15], and disseminated the standardisation work performed in the PQC4eMRTD project, as well as in the relevant RISC-V and ELISA working groups.

The presentation was an early version of the on-going work on the use of PQC in space processors and systems, which was eventually published in the IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT) 2026 conference [16], which was a candidate for the best paper award. This work performed an analysis of the CCSDS requirements on cyber security, and motivated the application and migration of cryptography to PQC in space systems. The work demonstrated experimentally that even legacy space processors are capable of executing PQC algorithms, and demonstrated that integration of PQC algorithms is possible in existing aerospace software, such as the National Aeronautics and Space Administration's (NASA) CryptoLib [17]. The resulting code has been released as open source [18].

Another presentation was performed in the IEEE Space Computing Conference, presenting the BSC developed QEMU emulation models of existing space processors [19]. The presentation included a PQC demo running on the METASAT platform [14] developed at BSC as part of the METASAT EU funded project [20] which is used in both the PQC4eMRTD and SMARTY [21] EU funded projects. The demo consisted of the secure communication between an FPGA implementing the METASAT platform and a QEMU emulator of the same platform. The demo was running on top of Linux and used the BSC developed ML-KEM and ML-DSA accelerators in both platforms, which exposed the functionality to the user space application using a Linux driver.

Finally, in September 2026, Dr. Leonidas Kosmidis delivered a keynote speech in the SafeComp 2026 conference in Valencia [22]. The presentation provided a summary of the research performed in the HADES (Hardware Dependability for Embedded Systems) group he is leading at BSC, which reconciles complex hardware and software with high assurance. The presentation highlighted the strong connection between safety and security, and the one on the security

aspect stressed the need for post-quantum cryptography migration, as well as standardisation, showing the benefits from the PQC4eMRTD project.

In addition to the aforementioned activities, Dr. Leonidas Kosmidis participated in two European Space Agency (ESA) standardisation efforts. The first one was in working group on the use of high-level and auto-coding hardware description languages for space, and the second one was in the Advanced Data Handling Architecture (ADHA). The hardware description working group was initially intended to become an ECSS group, however later it was changed to an internal SAVOIR working group within ESA. The announcement of the activity took place in 2024 [23] during the ADCSS (Avionics, Data, Control and Software Systems) workshop at ESA, in which Dr. Leonidas Kosmidis participated. The working group was established in 2025 and continued its meetings throughout 2026. Dr. Leonidas Kosmidis reported lessons learned through the use of high-level languages implementations of PQC algorithms, which have been developed and are being developed under his supervision with multiple tools. The working group has created a draft handbook which will become available once the working group has finalised its activities.

The latter is related to a standardisation activity of ESA in collaboration with European Space Industry for the development of an interoperable standard for payload computers. This defines a set of interfaces that allow the development of exchangeable compute modules for satellites. Dr. Leonidas Kosmidis is participating in the effort with the goal of ensuring encrypted transmissions within the satellite over ADHA interfaces. The working group is currently working on the definition of the ADHA 2.0 specification, following a set of plenary meetings during 2025 and 2026. Continuing in October 2026, four subcommittees have been formed, which will work on the specifications of each part, covering:

- Mechanical, Thermal and Electromagnetic Compatibility (EMC)
- System and Assembly, Integration, and Test (AIT)
- Electrical Interfaces
- Backplane connectors, Assembly

targeting the release of the specifications at the end of 2026.

4. Conclusion

In this deliverable we covered the participation in standardisation, as well as updates in standardisation either in newly created groups or about developments that happened after the delivery of the deliverable D2.2 [1].

Overall, considerable participation of the project members has been performed, mainly in various working groups of RISC-V, ELISA, Khronos and ESA standardisation activities. Moreover, the dissemination of the project in relevant safety critical venues, had the opportunity to motivate the migration to PQC in avionics and aerospace domains.

References

- [1] PQC4eMRTD, "D2.2 Report on the state of standardization for PQC, HPC and quantum computing," 2026.
- [2] RISC-V International, "RISC-V International Mailing Lists," [Online]. Available: <https://lists.riscv.org/g/main>.
- [3] RISC-V International, "RISC-V International Jira Spaces," [Online]. Available: <https://riscv.atlassian.net>.
- [4] L. Kosmidis, "Machine Readable Travel Documents: a Use Case for the PQC RISC-V TG," in *RISC-V North America 2025, Member's Day Presentation*, 2025.
- [5] S. Bogatell, A. Kapás, J. Castro Sisniegas, M. Bartoli, L. Migliari, P. Lukács, M. M. Trompouki and L. Kosmidis, "RISC-V PQC Hardware Implementations for Safe and Secure Systems: A Design Exploration," in *RISC-V Summit North America 2025, Poster Presentation*, 2025.
- [6] L. Kosmidis, "PQC4eMRTD: Post Quantum Cryptography for Resource Constrained RISC-V Systems," in *RISC-V Europe 2026, Poster Presentation*, 2026.
- [7] NIST, "Post-Quantum Cryptography," 2026. [Online]. Available: <https://www.nist.gov/pqc>.
- [8] RISC-V Space SIG, "Gap Analysis & The Transition to RISC-V," 2026. [Online]. Available: <https://riscv.atlassian.net/wiki/spaces/SPC/pages/1226801153/Gap+Analysis+The+Transition+to+RISC-V>.
- [9] RISC-V Space SIG, "RISC-V based Orbital Compute Data Center Pioneering the SPace-as-a-Service Revolution," 2026. [Online]. Available: <https://riscv.atlassian.net/wiki/spaces/SPC/pages/1880719378/RISC-V+based+Orbital+Compute+Data+Center+Pioneering+the+SPace-as-a-Service+Revolution>.
- [10] RISC-V Functional Safety SIG, "Functional Safety White Paper," 2025. [Online]. Available: <https://github.com/riscv/sig-functional-safety-whitepaper/releases#release-v1.0.0-prerelease-20251126>.
- [11] Ingonyama, "ICICLE GitHub Repository," 2026. [Online]. Available: <https://github.com/ingonyama-zk/icicle>.
- [12] RTCA/EASA, "Airworthiness Security Process Specification," 2020.
- [13] RTCA/EASA, "DO-355/ED-204A - Information Security Guidance for Continuing Airworthiness," 2020.

- [14] L. Kosmidis et al, "The METASAT Hardware Platform: A High-Performance Multicore, AI SIMD and GPU RISC-V Platform for On-board Processing," in *European Data Handling & Data Processing Conference (EDHPC)*, 2023.
- [15] L. Kosmidis, "Post Quantum Cryptography for RISC-V Space Systems," in *Flight Software Workshop*, 2026.
- [16] I. Fernandez Andonegui, M. Sole i Bonet, J. Wolf, M. M. Trompouki and L. Kosmidis, "Post Quantum Cryptography in Space Systems," in *IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, 2026.
- [17] NASA, "cFS Cryptography Library (CryptoLib) Open Source repository," 2022. [Online]. Available: <https://github.com/nasa/CryptoLib>.
- [18] I. Fernandez Andonegui and L. Kosmidis, "CryptoLib-PQC: Post-Quantum Cryptography integration for NASA's CryptoLib," 2026. [Online]. Available: <https://gitlab.bsc.es/ifernan2/CryptoLib>.
- [19] M. Solé, J. Wolf, A. Álvarez Suárez, M. M. Trompouki and L. Kosmidis, "Faithful Emulation of Space Processors SoCs using Open Source Technologies," in *Space Computing Conference (SCC)*, 2026.
- [20] L. Kosmidis et al, "METASAT: Modular Model-based Design and Testing for Applications in Satellites," in *Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS)*, 2023.
- [21] SMARTY, "Scalable and Quantum Resilient Heterogeneous Edge Computing enabling Trustworthy AI," 2024. [Online]. Available: <https://cordis.europa.eu/project/id/101140087>.
- [22] L. Kosmidis, "Combining High Performance Hardware and Software with High Software Assurance: Is it Possible?," in *Keynote at International Conference on Computer Safety, Reliability and Security (SafeComp) 2026*, 2026.
- [23] A. Urbon Aguado, "SAVOIR WG Handbook for auto-coding of HDLs for Space Applications," in *18th ESA Workshop on Avionics, Data, Control and Software Systems (ADCSS)*, 2024.