



Post-Quantum Cryptography for Automotive – Impact Assessment

An assessment of the potential security impact of the quantum threat on connected vehicles, and of the generic considerations for a transition to post-quantum cryptography across PC5 and Uu communications.

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to unlock the full power of connectivity so that people, industry and society thrive. Led by our members, we represent the interests of over 1,100 operators and businesses in the broader ecosystem. The GSMA also unites the industry at world-leading events, such as MWC (in Barcelona, Kigali, Las Vegas and Shanghai) and the M360 Series.

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

GSMA Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

GSMA's Antitrust Notice

The information contained herein has been prepared in accordance with the GSMA's Antitrust Policy: <https://legal.gsma.com/wp-content/uploads/2025/11/Antitrust-Policy-October-2025.pdf>

About the 5GAA

The 5G Automotive Association (5GAA) is a global, cross industry organisation of over 100 members, including leading global automakers, Tier-1 suppliers, mobile operators, semiconductor companies, and test equipment vendors. 5GAA members work together to develop end-to-end solutions for future mobility and transport services. 5GAA is committed to helping define and develop the next generation of connected mobility, automated vehicles, and intelligent transport solutions based on C-V2X. For more information, please visit <https://5gaa.org>

5GAA's Disclaimer

All Rights Reserved. No part may be reproduced except as authorised by written permission. The copyright and the foregoing restriction extend to reproduction in all media. This document has been prepared by the 5G Automotive Association (5GAA) and is based on the information and technology available at the time of its publication. It reflects the most current and accurate version to the best of 5GAA's knowledge. As technologies and industry standards continue to evolve, 5GAA is committed to regularly reviewing and updating this document as necessary to ensure its continued relevance.

Joint Ownership Notice

This document is jointly published and co-owned by the GSMA and the 5G Automotive Association (5GAA). All rights, including intellectual property rights, in this document are jointly held by both organisations. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means unless accompanied by full and accurate citation of this document, including its title, date of publication, and clear attribution to both the GSMA and 5GAA as joint authors. Any permitted use must reference this document in a manner that is prominent, unambiguous, and consistent with accepted citation standards. The views and recommendations expressed herein represent the agreed positions of both organisations.

© 2026 GSMA and 5GAA. All rights reserved.

Contents

Executive summary	1
1. Introduction	2
2. Abbreviations	3
3 Cryptography and the quantum threat	6
3.1. Symmetric algorithms, asymmetric algorithms and message encryption	6
3.2. Cryptographic authentication and integrity protection	6
3.3. The quantum threat	7
3.4. PQC algorithms and regional approaches	8
3.5. The risk to automotive communications	10
4. 5GAA OEMs' position on potential impact and post-quantum cryptography strategy	11
4.1. Introduction	11
4.2. PQC and the evolution of connected vehicles	11
4.3. Systems and use-case classes potentially impacted	13
4.4. Qualitative consequence categories	13
4.5. Supply chain and ecosystem implications	14
4.6. External dependencies: standards, policy, and regulatory context	14
4.7. Summary statement	15
5. Technical analysis to support automotive-specific post-quantum cryptography strategy	16
5.1. Connected automotive system	16
5.2. PC5-based systems	17
5.2.1. Implications for 3GPP PC5 and NG-PC5	17
5.2.2. V2X-Direct application taxonomy	18
5.2.3. Types of cryptographic overhead	26
5.2.4. Conclusions	27
5.3. Uu-based systems	27
5.3.1. PQC and mobile telecommunications	27
5.3.2. Impact of quantum-safe strategies on mobile network capacity & efficiency	29
6. Conclusions and next steps	30
7. References	31

Executive summary

Continued advances in quantum computing technologies pose an emerging threat to widely deployed cryptographic methods, which underpin the security assurances necessary for many modern forms of communications. This document provides an assessment of the potential security impact of this quantum threat on connected vehicles, discussing the vulnerability of currently deployed asymmetric cryptographic algorithms, and outlining generic considerations for the transition to postquantum cryptography (PQC; namely new algorithms intended to protect against the threat).

In the context of automotive vehicle communication systems, particularly PC5 (direct V2X) and Uu (cellular) interfaces, the adoption of PQC may affect system characteristics such as computational load, message size, latency, and network efficiency. PQC algorithms typically introduce additional overhead and may require adaptations to existing protocols and system architectures. There will be a legacy fleet of intelligent vehicles which remain vulnerable to quantum attack, one objective of the industry is to minimise the size of this legacy fleet. Older (current) vehicles will not be susceptible to attack whereas future vehicles will be equipped with post-quantum systems, either during production or via post-retail techniques, i.e. Over-the Air (OTA) update.

A qualitative industry perspective, from key 5GAA Automotive industry members is presented, highlighting considerations associated with long vehicle lifecycles, legacy system constraints, and varying levels of upgradeability across fleets. It identifies a range of connected vehicle use cases that may be affected and discusses broader elements such as supply chain coordination, standardisation, and regulatory alignment. Overall, the document highlights the need for a structured and coordinated approach to support the gradual transition towards quantumresilient automotive communication systems, acknowledging the commercial environment in which OEMs operate, which to some extent defines industry strategies going forward as co-ordinated but independent.



1. Introduction

The emergence of quantum computing presents a fundamental challenge to the cryptographic mechanisms that underpin modern digital systems, including those used across connected and automated vehicle ecosystems. Widely deployed asymmetric cryptographic algorithms, which provide key exchange, authentication, encryption and digital signing capabilities, are expected to become vulnerable once sufficiently powerful quantum computers emerge. While symmetric cryptographic techniques can be adapted to maintain security through parameter adjustments, asymmetric schemes require replacement by standardised quantumresistant alternatives, driving the need for a structured transition to postquantum cryptography (PQC).

Within the automotive domain, this transition is particularly complex due to the long lifecycles of vehicles, the diversity of connected use cases, and the tight performance constraints associated with realtime and safetycritical communications. Connected vehicle systems rely on multiple communication modes, including direct (PC5) and networkbased (Uu) interfaces, each with distinct operational and architectural characteristics. The introduction of PQC is expected to introduce additional computational overhead, larger key and message sizes, and potential impacts on latency, bandwidth efficiency, and system scalability. This document provides a technical analysis of these impacts, focusing on how PQC adoption affects automotive communication systems and supporting the development of an automotivespecific strategy for transitioning to quantumsafe cryptography. It includes a summary of the collective position of 5GAA

automotive OEM members regarding the well-understood need to transition to quantum-resilient systems in the future and the way forward based on the industry's common approach to adapting their respective systems in the context of a commercially competitive environment.

This work has been undertaken by the 5GAA within its partnership with the GSMA, defined by MoU. The scope of this work has been limited to the analysis of automotive connectivity requirements for post-quantum resilience only. Operational and business support systems are not considered here.

2. Abbreviations

Term	Description
AES	Advanced Encryption Standard
ADAS	Advanced Driver Assistance Systems
AKA	Authentication and Key Agreement
BSM	Basic Safety Message (SAE)
CAM	Cooperative Awareness Message (ETSI)
CITS	Cooperative Intelligent Transport Systems
CRQC	Cryptographically Relevant Quantum Computer
CSP	Communications Service Provider
DENM	Decentralised Environmental Notification Message (ETSI)
EC / ECC	Elliptic Curve / Elliptic Curve Cryptography
ECU	Electronic Control Unit
EPSAKA	Evolved Packet System Authentication and Key Agreement
EU	European Union
FNDSA	Falcon Digital Signature Algorithm
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GSMA	Global System for Mobile Communications Association
HQC	Hamming Quasi-Cyclic (Key Encapsulation Mechanism)
IKEv2	Internet Key Exchange version 2
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
JTAG	Joint Test Action Group
KEM	Key Encapsulation Mechanism
MAC	Message Authentication Code

Term	Description
MLDSA	Module Lattice Digital Signature Algorithm
MLKEM	Module Lattice Key Encapsulation Mechanism
MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
NGPC5	Next Generation PC5 (sidelink interface evolution)
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OSNMA	Open Service Navigation Message Authentication
OTA	Over-The-Air
PC5	3GPP sidelink interface for direct UE-to-UE communication
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PRINS	Protecting Roaming using an Integrated Network Security solution
RAN	Radio Access Network
RSU	Roadside Unit
RSA	Rivest-Shamir-Adleman (public-key cryptosystem)
SDV	Software Defined Vehicles
SEPP	Security Edge Protection Proxy
SLHDSA	Stateless Hash-based Digital Signature Algorithm
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SUPI	Subscription Permanent Identifier
SUCI	Subscription Concealed Identifier
TCU	Telematics Control Unit
TIM	Traveller Information Message
TLS	Transport Layer Security
TUAK	TUAK Authentication Algorithm (3GPP authentication algorithm)
UE	User Equipment

Term	Description
Uu	Cellular interface between UE and base station (3GPP)
USIM	Universal Subscriber Identity Module
V2X	Vehicle-to-Everything
VPN	Virtual Private Network

3. Cryptography and the quantum threat

3.1 Symmetric algorithms, asymmetric algorithms and message encryption

Cryptographers sometimes distinguish between two categories of algorithms, namely symmetric cryptographic algorithms, in which both parties in a communication use the same key, and asymmetric or public key cryptographic algorithms, which require the sender and recipient of an encrypted communication to use distinct keys. A widely deployed example of a symmetric algorithm is the Advanced Encryption Standard (AES), which is a standardised algorithm for encrypting messages. When using AES, the sender who encrypts a message and the recipient who decrypts the ciphertext both use the same key. Symmetric algorithms are typically very efficient, which is one reason for their widespread adoption, but have the drawback that the communicating parties must agree or share the secret key prior to commencing the communication.

For many instances, such as when the communicating parties are geographically separated or there are many different pairs of communicating parties, establishing these shared keys directly, e.g., by meeting in person or agreeing keys prior to the communication, is impractical or infeasible. This bottleneck is overcome by using asymmetric algorithms, in which each communicating entity or individual has their own public key and their own private or secret key. An individual's public key can be made publicly available, and other parties may use the public key to encrypt a message intended for that individual. However, only the owner of the corresponding secret key can decrypt the encrypted message. Such methods are generally more expensive, in terms of execution time or computational overhead, however, they offer great flexibility since any arbitrary pair of communicating entities can easily exchange confidential messages. In practice, asymmetric methods are typically used at the beginning of a communication, to establish a shared symmetric key, which the communicating parties then use to encrypt messages with symmetric algorithms – this combined approach leverages the flexibility of the asymmetric methods and the performance advantage of the symmetric methods.

3.2 Cryptographic authentication and integrity protection

Cryptography is also used to achieve message integrity and authentication: a sender can use an “authentication tag creation key” to generate a tag on a message such that a receiver can use an “authentication tag verification key” to check that the tag on the message was generated by someone who knows the tag creation key (giving authentication) and that the message hasn't been changed since the tag was generated (giving integrity). As with encryption, there are symmetric and asymmetric forms for integrity and authentication. In the symmetric form, the tag is called a message authentication code (MAC) and the creation and verification keys are the same as each other, so both the sender and receiver know the same key. In the asymmetric form, the tag is called a signature, the creation key is a private key, and the verification key is a public key. As with encryption, the symmetric and asymmetric forms have different strengths: symmetric authentication is faster and has smaller tags but requires agreement on the symmetric key and allows the receiver to create a message tag and claim it was generated by the sender; asymmetric authentication is slower and typically has larger tags but can be carried out between two parties that have no existing relationship and has the property of non-repudiation, where only the valid sender's key could have created the signature and the receiver cannot create a forgery. In the V2X broadcast setting, with a large and changing population of potential receivers, signatures on messages are the most natural way to provide authentication because it is impractical to pre-establish symmetric keys with all potential receivers.

3.3 The quantum threat

A cryptographically relevant quantum computer (CRQC) is a quantum computer that possesses sufficient size and accuracy to execute quantum algorithms at the scale needed to attack deployed cryptographic algorithms. CRQCs do not yet exist, since present-day quantum computers are neither sufficiently large nor precise to execute the relevant quantum algorithms at cryptographically relevant scales. However, quantum computers are rapidly evolving and, when CRQCs do emerge, the impact of such attacks will depend on the type of cryptographic method considered.

Symmetric cryptographic algorithms such as AES may be vulnerable to attacks that use a CRQC to execute Grover's algorithm, a quantum version of the generic needle-in-a-haystack search, that does not leverage any structure in a problem, treating it in a black box fashion. Relative to traditional methods, in theory, Grover's algorithm achieves a quadratic speedup. However, the algorithm is considered more futuristic, in the sense that deep circuits are required, and additionally it cannot be parallelised with the same efficacy as traditional algorithms, making the extent to which the speedup will be realised in practice less clear. Many national expert bodies are currently (as of August 2025) recommending that Grover's algorithm does not require any change to symmetric algorithms. Nonetheless, even if the theoretical quadratic speedup were fully realised, security assurances could be maintained with existing methods by doubling the key length. For most mobile network contexts, doubling the key length for symmetric algorithms is considered manageable, in terms of complying with performance constraints. Indeed, standardisation work on bespoke telco-sector algorithms that rely on symmetric cryptography, such as the algorithms that provide confidentiality and message integrity over the radio interface (e.g., SNOW) and the authentication and key agreement algorithms (e.g., MILENAGE), is already underway. The updated versions of these algorithms increase the security assurance from 128-bits to 256-bits (approximately), in line with the doubling of security that would in any case provide assurances against Grover-based attacks.

Contrary to symmetric algorithms, quantum computers pose a significant threat to current asymmetric cryptographic algorithms, such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) methods. These algorithms rely on mathematical problems that are computationally hard for classical computers—like factoring large integers (RSA) or solving the discrete logarithm problem (ECC). However, quantum computers can solve these problems efficiently using Shor's algorithm, which runs in polynomial time on a sufficiently powerful quantum machine. This means that once large-scale quantum computers become practical, they could break the algorithms currently used in many secure communications protocols and methods, including TLS, IPsec VPNs, and digital signatures. The threat is especially serious for long-lived data or systems that require forward secrecy, because encrypted data captured today could be

decrypted in the future once quantum capabilities mature. More generally, the use of asymmetric digital signatures and key exchange methods will ultimately be vulnerable to quantum-based attacks once a CRQC emerges, irrespective of the data shelf-life.

Important to note, as mentioned in the previous paragraph, that in many cases symmetric keys are shared using asymmetric methods. The implication is that if the asymmetric methods were to be compromised then the security of the symmetric keys they protect is also effectively compromised. Note that, in the present context, many V2X use cases, such as safety and mobility use cases, do not use confidential information and make use of information with a very short active or relevant lifetime (i.e., short-lived data), so this "harvest-and-decrypt" attack, while important for internet commerce and protecting long-lived data such as corporate IP, is not the main concern for V2X. However, other car connectivity use cases such as financial interactions or upload of personal information for insurance purposes may feature data that is of use to an attacker for some time and so may be potential targets for this type of attack. The general threat to digital signature schemes and asymmetric key exchange methods posed by quantum computing will apply to all sectors that use these methods, including V2X.

3.4 PQC algorithms and regional approachest

Although symmetric algorithms like AES are more resistant—requiring at most a doubling of key sizes to remain secure—asymmetric algorithms must be replaced entirely. This has led to the development of post-quantum cryptography (PQC), which uses quantum-resistant mathematical problems, such as lattice-based or code-based schemes. Standards bodies like INIST or ISO are actively working to standardize PQC algorithms to ensure



a smooth transition before quantum computers become a practical threat and a first set of standardised algorithms has been finalised. The NIST PQC standardization process began in 2016 and has progressed through multiple rounds of evaluation, culminating in the fourth round in early 2025. As of 2025, NIST has finalized the selection of several post-quantum cryptographic (PQC) algorithms to replace or supplement classical public-key cryptography in the face of the quantum threat. The PQC algorithms are designed to be secure against attacks from quantum computers, which could break widely used schemes like RSA and ECC. The first group of standardized algorithms includes ML-KEM, a key encapsulation mechanism (KEM), and ML-DSA, FN-DSA, and SLH-DSA for digital signatures. ML-KEM (submitted to NIST under the name CRYSTALS-Kyber; standardised as FIPS 203) is intended for secure key exchange in protocols like TLS, IPsec VPNs, and encrypted messaging. ML-DSA (submitted to NIST under the name CRYSTALS-Dilithium; standardised as FIPS 204) and FN-DSA (submitted as falcon; to be standardised as FIPS 206) offer efficient and compact digital signatures suitable for software updates, identity verification, and secure boot processes. SLH-DSA (submitted as SPHINCS+; standardised as FIPS 205), while slower, provides a stateless hash-based alternative with strong security assurances. In March 2025, NIST also selected HQC (Hamming Quasi-Cyclic) as a second KEM, to be standardised, expanding the diversity of cryptographic foundations beyond lattices.

NIST is currently drafting formal standards for HQC and other selected algorithms, which will be released for public comment before final publication—expected within two years. Meanwhile, NIST continues to evaluate additional signature schemes through an on-ramp process, seeking alternatives that are not based on structured lattices and offer short signatures with fast verification. These efforts aim to ensure cryptographic diversity and resilience. NIST is also working with international bodies like ISO to align standards and facilitate global adoption. Algorithms selected by NIST are anticipated to be widely deployed, though other jurisdictions such as South Korea and China will also select their own preferred algorithms for standardisation.

The ISO/IEC framework has established a comprehensive, multi-layered draft blueprint partitioning PQC standards into distinct basic primitives. For key encapsulation and asymmetric ciphers, ISO/IEC is incorporating a diverse portfolio into ISO/IEC 18033-2/AMD, which integrates the code-based Classic McEliece KEM, the LWE-based FrodoKEM, and structured module-lattice schemes

including ML-KEM-768 and ML-KEM-1024 (explicitly excluding security level 1 mechanisms like ML-KEM-512). Digital signature primitives are similarly granularized: stateful hash-based alternatives XMSS and LMS are finalized under ISO/IEC 14888-4, while ML-DSA and SLH-DSA are steadily advancing through ISO/IEC 14888-5 (WD) and ISO/IEC 14888-6 (CD) respectively. Crucially, the classic lattice-based mechanism NTRU has been allocated to the lightweight cryptography framework under ISO/IEC 29192-4/AMD. To ensure the implementation correctness and security of these regional and international PQC algorithms, ISO/IEC is concurrently advancing the revision of ISO/IEC 18367 (currently progressing as a Working Draft). This standard establishes the universal baseline for cryptographic algorithms and security mechanisms conformance testing.



In China, the National Cryptography Administration (NCA) and the Chinese Association for Cryptologic Research (CACR) govern an independent selection process. Sovereign deployments prioritize native quantum-resistant entries to build an algorithmic defense line. These include lattice-based primitives such as LAC (a key encapsulation mechanism) and Aegis (a digital signature), supplemented by multivariate and alternative mathematical designs like Huafu.

In Japan, the CRYPTREC committee (established by MIC and METI) and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) drive the domestic PQC transition, mandating complete government and telecommunications migration by 2035 to mitigate "harvest-now-decrypt-later" threats. Notably, Japanese cryptographic expert groups have been primary international proponents of the NTRU framework, spearheading its parameters and security tuning to secure its inclusion in the lightweight ISO/IEC 29192-4/AMD track.

In South Korea, the National Intelligence Service (NIS) and the National Security Research Institute (NSR) enforce an entirely separate, sovereign suite of algorithms via the Korean Post-Quantum Cryptography (KpqC) initiative. Legally embedded within the KCMVP 3.0 (Korea Cryptographic Module Verification Program) validation framework, South Korea requires native support for four localized algorithms: SMAUG-T and NTRU+ (an advanced domestic variant of the NTRU lattice structure) for key encapsulation, alongside HAETAE and AIMer (a symmetric-key-based digital signature) for authentication.

Meanwhile, European cybersecurity directives, harmonized across agencies like Germany's BSI and France's ANSSI, mandate strict cryptographic diversity and hybrid deployment models¹ to hedge against single-point-of-failure risks in structured lattices. Specifically, European frameworks actively prioritize Germany's FrodoKEM (unstructured lattice-based) and the Netherlands' Classic McEliece KEM (code-based) as the primary non-NIST alternative KEMs for high-assurance applications.

Regarding performance characteristics, several new PQC algorithms are as fast (or even more) as the current asymmetric algorithms, even though some require more compute time to execute. However, they use larger parameters (public key, ciphertext, signature) compared to the classical asymmetric algorithms in some cases, the overhead is not particularly onerous, and the algorithms can largely serve as drop-in replacements, although, in other cases redesign may be required. However, this is a context dependent matter requiring one to assess the performance characteristics of the new algorithms against the requirements of the use case, to determine the viability of using the algorithm and the complexity of migrating to PQC. At present, this matter is complicated by the fact that standardisation remains ongoing, and the performance characteristics of to-be-standardised algorithms may differ from those already standardised. Making decisions on which PQC algorithms to use for a given use case and assessing the anticipated complexity of migration will ultimately depend on which algorithms are standardised.

¹ In the context of PQC migration, hybrid cryptography refers to methods that combine a traditional algorithm (such as an elliptic curve method) with a PQC algorithm. This approach adds protection against quantum attacks but also maintains traditional protection in case of unforeseen issues with a newer PQC algorithm (e.g., implementation errors), ensuring that security is not inadvertently reduced during migration

3.5 The risk to automotive communications

PQC transition spans three distinct domains: (i) Enterprise IT systems, (ii) Vehicle Connectivity Data Platform as the controlled interface between backend and vehicle, and (iii) invehicle systems. However, the scope of the work represented here is limited to the implications of post-quantum cryptographic solutions on the underlying communications modes (Uu, PC5) for implementation in the automotive industry.

The urgency of migrating to PQC is not just theoretical—nation-states, for example, may already be harvesting encrypted data in anticipation of future decryption, the strategy known as “harvest now, decrypt later” (HN,DL). Therefore, transitioning to quantum-safe cryptography is a critical step in securing digital infrastructure for the coming decades. The HN, DL attack motivates a near-term migration to quantum safe cryptography in certain contexts since the attack may be relevant prior to the emergence of an adequately large quantum computer, when considering data with a long-lived shelf life. When organisations assess the quantum threat, assets that communicate confidential long-lived data are typically considered as higher risk, owing to the HN, DL attack. Additionally, the implementation of new, quantum resistant algorithms is not a straightforward replacement, it is likely to be a multi-year transition that will have implications across the full enterprise stack: for this reason, leveraging technology refresh cycles and future proofing roadmaps is critical to enabling a PQC transition.

Mitigating against future (quasi) real time attacks, namely attacks which require an active CRQC to execute, such as forging a signature to break an ongoing authentication process, may seem less pressing relative to protecting against the HN,DL attack (since the latter may already be relevant now). However, in addition to considering the data shelf-life, when assessing the risk associated with an asset, one must also consider the migration time required to make the asset quantum safe. If the asset can be migrated with a simple software update, for example, the risk is considered lower since there should be adequate time to perform such a migration before a CRQC emerges. But if migration requires a longer timeframe, the likelihood increases that a CRQC emerges before the asset is migrated. Thus, both migration complexity and data longevity are factors that can increase the risk associated with an asset.

There are multiple categories of assets that could require a long migration time. One category includes complex assets or systems, including infrastructure such as a telecommunications network, which involve many components and will require considerable time to migrate. Complex assets or systems of assets will require considerable planning to migrate. This can include assets relying on an underlying public key infrastructure (PKI), since migrating a full PKI is expected to be an involved process.

Another category of assets that can present a higher risk are those requiring new protocols or standards to be developed, to accommodate the heavier performance of the new PQC algorithms. If the performance profile of the new PQC algorithms is not compatible with existing performance constraints or protocol requirements, the migration time will be elongated by the need to first design protocols that can accommodate the PQC algorithms. Examples here include constrained environments where resources are limited such as IoT devices with compute constraints or communication protocols with bandwidth limitations.

A third category of higher risk assets includes long-lived hardware assets with embedded quantum-vulnerable cryptographic algorithms. If such assets remain active in the field when quantum capabilities mature, new attack vectors will be available. Examples include embedded hardware with cryptography, used for secure boot or for managing security checks associated with software updates, within long lived vehicle ecosystems that may extend beyond the lifetime of individual vehicles.

The above shows that multiple factors influence the complexity of migration and the risk associated with an asset. The type of data communicated, the life cycle of the asset, and the overall complexity of the asset need to be considered. So too the dependence of the asset on protocols and standards, and the viability of using PQC algorithms within these protocols/standards. The matter is complicated further by the fact that standardisation of PQC algorithms themselves remains ongoing.

Different countries and regions are developing specific post quantum migration plans. For example, the EU recommends that by the end of 2026, member states identify use cases where cryptographically relevant quantum computers would create high or medium risk, and initiate transition planning for those use cases. At the time of writing, it is not known which (if any) automotive use cases would be considered high or medium risk.



4. 5GAA OEMs' position on potential impact and post-quantum cryptography strategy

4.1. Introduction

In this section 5GAA automotive OEMs present a qualitative industry view of how cryptographically relevant quantum computing could affect connected systems in production vehicles and the associated industry effort required for a transition to post-quantum cryptography (PQC). The aim is to raise awareness and reassurance without disclosing implementation details, prioritisation decisions, milestones, or other sensitive information, and is limited in scope to vehicle-resident applications that communicate with external endpoints (including Uu and PC5 connectivity). It explicitly excludes details of OEM internal IT/back-end architectures, proprietary security programmes, supplier identities or any detail that could reveal subsystem prioritisation and be exploitable if disclosed. This document does not expose exploitable sub-system level detail on OEM system architecture or cryptographic implementation.



4.2. PQC and the evolution of connected vehicles

The core challenge is that future quantum capabilities may compromise today's widely deployed public key cryptography, which is a foundational dependency for authentication, trust establishment, key exchange (encryption) and signing across many connected-vehicle functions. The impact of such a compromise could include effects on vehicle functionality, safety-related services, privacy, and OEM operational/brand risk.

At the same time, OEMs face a structurally different challenge than many IT domains because automotive platforms and derivatives have long development and in-field lifecycles; vehicles on the road today often originate from architectures-initiated years earlier. This so-called legacy fleet reality strongly shapes feasible migration approaches and the urgency of implementing a "crypto-agile" design in new platforms.

The unknown timeline associated with the expected emergence of the quantum-enabled cryptography threat and the evolving system and functional architecture of production vehicles creates now and will create in the future a complex legacy fleet characteristic to be considered. We can think of the vehicle legacy fleet as a set of three connected-vehicle generations that have emerged and will emerge as a function of time and installed vehicle capability. The expected threat to each connected-vehicle generation varies with their connectedness, capability and flexibility. Firstly, there is a connected-vehicle generation of older legacy vehicles, mostly already on the road today, with limited connectedness and minimal service functionality. These are not considered significantly vulnerable to quantum threats due to the lack of attack vectors and low-level consequences (i.e. gains for the attacker) that might occur after compromise. They are very low-level targets for quantum attackers, and very little in terms of a post-quantum strategy is expected to be required for these vehicles.

Those legacy vehicles are not considered high-value quantum targets due to the absence of meaningful attack vectors.

A second generation comprises smarter vehicles, with more connected or remote functionality which use pre-quantum (classical) techniques for cryptography and other related functions. These vehicles which are emerging from production lines today, have very little flexibility for post-sales cryptography upgrade even after solutions for the post-quantum threat has been agreed and standardised. A strategy to upgrade these vehicles would be extremely complex and costly for vehicle manufacturers and vehicle owners. Customers are not expected to accept any permanent loss of their vehicle's functional performance, resulting from any shut-down implemented to minimise the consequences of a quantum-enabled compromise for the sake of a secure vehicle. This is the main 'legacy dilemma' facing the industry today.

The third connected-vehicle generation comprises even smarter vehicles with flexible software-based systems supporting the capability to upgrade pre-quantum cryptography systems over the air, or during routine servicing, without the need for hardware update. This vehicle type will demonstrate the increasing importance of Software defined vehicles (SDV)-based and AI-based services, which will lead to even higher dependencies on off-board functions and will require high-level KPIs in the network link/connectivity. We can expect that these vehicles will emerge from among the higher-end vehicle models being produced in the foreseeable future, and that such technology to 'trickle down' to more affordable models once it matures and reduces in cost. The post-quantum strategy for such vehicles could involve a temporary restriction of vehicle capability or performance until the software upgrade is agreed and implemented.

Often, in legacy vehicles migration approaches are not realistic. In particular, former eco systems/tool chains for outdated electronic platforms are no longer available and loss of know-how would increase efforts to unrealistic levels.

A challenge for manufacturers today is to minimise the number of vehicles belonging to the second generation by accelerating the introduction and production of vehicles in the third generation. An important factor in achieving this transition from the second to the third generation is to prioritise cryptoagility, particularly in key components. Cryptoagility refers to design choices that ensure an ability to easily update or change cryptographic algorithms after deployment, in response to e.g. the evolving standardisation or threat landscape. The ability to migrate cryptographic methods after vehicle sales would ideally be incorporated into component design to enable more vehicles to join the third generation and reduce the risk associated with non-updatable legacy vehicles/systems. A key element for achieving this cryptoagility will be to work on supply chain requirements to minimise the number of systems that fall into the "not upgradeable" category.



4.3. Systems and use-case classes potentially impacted

The following connected-vehicle system classes are representative of where PQC transition considerations arise:

Connected vehicle / external comms use cases

- Telematics (vehicle ↔ OEM backend services)
- C-ITS / V2X information and safety messaging (non-ADAS and emergency braking contexts)
- ADAS-connected safety functions that depend on external communications
- Core vehicle software update / OTA / software-defined vehicle services
- Infotainment, navigation, in-car internet access / Wi-Fi hotspot
- Plug and charge ecosystem / increasing importance of resilient integration of electric vehicles into the energy storage and distribution system
- eCall (mandated + OEM-provided extensions)
- Vehicle tracking / theft prevention / fleet management
- Remote services (e.g., remote access, remote assistance/piloting)
- Payments / tolling / related third-party services
- Digital key / device-to-vehicle trust (e.g., phone-as-key ecosystems)
- GNSS augmentation / authenticity validation where applicable
- Cross-cutting security and lifecycle mechanisms (often embedded across many use cases)
- Secure boot / platform integrity mechanisms (boot time constraints frequently apply)
- Software Integrity Protection during execution
- ECU code signing and update software/firmware authenticity (e.g., OTA and maintenance flows)
- Device/vehicle identity and credentialing (incl. certificates, provisioning)
- Secure diagnostics / maintenance access control (incl. debug access patterns)
- Secure storage and integrity of critical data at rest

4.4 Qualitative consequence categories

Impacts vary by use case but can be described at a category level without detailing individual vulnerabilities. The following categories are commonly used in qualitative assessments:

- **Safety and road-risk consequences:** degradation of safety-relevant connected functions could increase real-world harm potential.
- **Security of vehicle functions and services:** loss of authenticity/integrity assurances can undermine trust in vehicle-to-X communications and remote services.
- **Privacy and personal data exposure:** compromised cryptographic protections can raise privacy risks where personal/vehicle data is exchanged externally.
- **OEM operational and brand impact:** reputational harm, incident response burden, potential service disruption or recalls are plausible categories of consequence.
- **Ecosystem/third-party impacts:** third-party services (payments, charging, connectivity partners) can be affected across the end-to-end chain, as highlighted in questions about the broader ICT chain and target audience.
- Financial risks due to regulatory non-compliance, for example GDPR, Data Act, Digital Service Act.

4.5. Supply chain and ecosystem implications

Automotive connected systems are delivered through multi-tier supply chains. OEMs retain a commitment to customers and are accountable to regulators, while PQC-readiness typically involves coordination across Tier-1 and deeper supplier components. OEMs stressed that OEM responsibility remains, while acknowledging the need to engage the supplier community and specialised security members, without exposing specific supplier relationships.

It was noted that a recent BSI-hosted workstream discussion also identified “migration management across supply chain” as a prominent cross-sector theme, reinforcing that supply-chain coordination is a widely recognised part of PQC transition planning. Some resulting implications are

- Automotive OEMs and their suppliers will need aligned terminology, interfaces, and expectations for PQC capability evolution (often best addressed via standards and common profiles rather than bespoke approaches).
- OEMs are working internally on their prioritisation, therefore public materials should focus on shared challenges (lifecycle, performance constraints, certification needs) rather than “what will be fixed first.”

4.6 External dependencies: standards, policy, and regulatory context

Post-quantum cryptography (PQC) deployment is increasingly emerging as a cross-cutting policy and compliance priority worldwide. Most major jurisdictions have adopted or are developing national PQC transition strategies, reflecting growing concerns about the long-term security of current cryptographic systems and the need to prepare for future quantum-enabled threats. While timelines vary, there is broad convergence around inventory, planning and migration preparation activities, with many governments targeting migration of priority systems by around 2030 and broader adoption during the 2030–2035 timeframe.

Although these initiatives vary in scope and implementation, they generally do not create standalone PQC obligations. Instead, they tend to integrate quantum-readiness considerations into existing cybersecurity, data protection, critical infrastructure and resilience frameworks. As a result, organisations are increasingly encouraged to inventory cryptographic assets, assess quantum-related risks, develop migration roadmaps and adopt cryptographic agility as part of broader risk-management programmes. Data protection frameworks may further reinforce these expectations by requiring appropriate technical measures to ensure the long-term protection of personal data, including against risks associated with “harvest now, decrypt later” attacks².

Moreover, these developments remain largely horizontal rather than sector-specific. Concerning automotive, while South Korea has included intelligent transport system (ITS) infrastructure among the sectors covered by PQC migration pilots, governments have not yet prioritised PQC regulations or initiatives specifically targeting connected vehicles.

An additional complexity lies in meeting regulatory requirements across different geographies that may have contrasting positions on aspects of PQC implementation. As an example, the use of hybrid cryptography is one such topics where regulatory positions vary.

OEMs note that, although public visibility of PQC migration expectations is increasing, the automotive supplier community may not yet see consistent flow-down requirements. Currently, automotive stakeholders are therefore more likely to be affected indirectly through broader cybersecurity, critical infrastructure, procurement and supply-chain requirements than through dedicated automotive PQC regulation, though this situation might evolve.

In this context, authorities may support the automotive PQC transition by providing:

- Clear, stable standardisation signals (so implementations can converge rather than fragment);
- Clear signals on the direction of future requirements;
- Guidance on acceptable assurance approaches (e.g. evaluation and certification expectations) without mandating a single proprietary solution;
- Cross-border alignment to reduce regional fragmentation, particularly for globally produced vehicles;
- Practical transition guidance that recognises long vehicle lifecycles and legacy fleet realities; and
- Test and validation opportunities that enable confidence-building without disclosing sensitive implementation details

² See GSMA PQC Government initiatives tracker for an overview of policy development worldwide. Available [here](#).



4.7 Summary statement

OEMs and the broader automotive ecosystem recognise the need to prepare connected-vehicle systems for a future in which quantum computing could undermine today's public-key cryptographic foundations. While public disclosure of subsystem-specific priorities and detailed implementation approaches is not appropriate due to cyber risk and competitive sensitivity, the industry is actively engaging with suppliers, standards bodies, and authorities to contribute to ecosystem readiness for PQC transition and cryptographic agility in future vehicle systems, consistent with the automotive sector's long development and infield lifecycles.

Individual prioritization by the OEM will occur according to a manifold of different potential decision parameters like: Estimation of timing and extent of progress in quantum computing, individual risk analysis, internal and external development resources, generic platform strategies on component/system/vehicle level, cost estimations, supply-chain considerations, etc.]

5. Technical analysis to support automotive-specific post-quantum cryptography strategy

5.1 Connected automotive systems

In the context of connected automotive, the quantum threat can be relevant to the communications methods and to some systems within the vehicles themselves. We first consider automotive specific use cases which are in the domain of Connected Vehicle (communication with vehicle-external services/entities). PQC-relevant aspects are of a technical nature. We have compiled a list of automotive use cases that should be included when considering a PQC strategy and have included use-case specific notes of interest. The list is intended to be indicative, demonstrating the nature of the challenge, but does not claim to be exhaustive.

- Generic V2X direct communications. Secure authentication for V2X is now based on EC or RSA cryptography.
- Secure Boot. It is important to keep the boot time as short as possible. The performance profile of PQC digital signatures differs to that of traditional (EC or RSA) methods, which could impact secure boot.
- Over-the-air (OTA) software updates (specified in ISO 24089 as well as R156)
- Public Charging (ISO 15118-2/20, AutoCharge, Plug and Charge)
- ECU code signing, needs to conform to ISO 21434, UNECE R155/156, GB44495/GB44496 (China) etc. There are other symmetric issues that should not be conflated, but just recorded for completeness: i.e AutoSar SecOC
- CCC (Car Connectivity Consortium) Phone as Digital Key
- JTAG (Joint Test Action Group) Unlock to allow debug access to the chips of the car in case of problems. Today it is based challenge/response mechanisms on RSA or EC crypto.
- Secure diagnostics 0X29
- Secure Storage: signature is based on EC or RSA cryptography.
- Infotainment Storage
- Driver authentication by means of biometrics/digital key
- MIPI high bandwidth video
- IoT services, such as electric pre-heating of the vehicle seats, cabin, engine (ICE and electric) etc.
- L-band GNSS augmentation/correction services authenticity verification is now based on EC or RSA cryptography. It is important to keep the signature size as little as possible.
- Galileo OSNMA TESLA root key distribution is protected via EC cryptography. It is important to keep the signature size as little as possible.
- Data transfer from TCU to the vehicle manufacturer's backend systems. Some OEMs use TLS v1.2 for transmitting telemetry data over the Internet. This method will be impacted.
- Telemetry data transfer from the car's TCU over a VPN tunnel between the MNO and the OEM's backend Site-to-site VPNs will be affected.
- Over-the-air control mechanisms. If IP-based wake-up mechanisms are used, they could be impacted.
- Mobile apps of OEMs. These mostly use HTTPS with TLS, meaning app traffic will be affected.
- Remote SIM provisioning mechanisms. In some countries, RSP is almost mandatory for OEMs. If a car is imported, local MNO SIM profiles must be activated within a certain period. During the RSP process, GSMA-defined security mechanisms are used. These mechanisms are currently not secure against post-quantum attacks.
- Other MNO-related quantum impacts → Algorithms related to radio network integrity, confidentiality protection, and SUPI concealment.

5.2. PC5-based systems

The quantum threat also impacts the communications methods used by connected vehicles. In what follows, we first discuss some of the key impacts of introducing PQC; these must be assessed to ensure that PQC solutions satisfy performance requirements for connected vehicle communications. The subsequent subsections outline some relevant implications for 3GPP PC5 and NG-PC5, and provide, as example, a detailed case study for V2X-Direct communications, indicating the nature of the threat and the impact for the different categories of V2X-Direct communications.

Increased computational and communication overhead

Post-quantum cryptographic algorithms are not a transparent replacement for classical algorithms from a performance perspective and can involve:

Larger key sizes and signatures: These increase the payload size of security-related messages (e.g. authentication, authorisation), which can reduce spectral efficiency on PC5 links—especially in congested V2X environments

Higher processing demands: Devices using PC5 (e.g. OBUs, RSUs) often have constrained compute and power budgets. Implementing PQC may require hardware upgrades or optimised firmware to maintain real-time performance

Latency and Throughput Trade-offs

Latency: Protocols that incur overhead due to the introduction of PQC algorithms could increase latency and impact connectivity

Reduced throughput: The overhead from PQC can reduce the effective data rate, particularly in scenarios with frequent re-authentication or secure message exchanges (e.g. CAM/DENM in V2X)

The performance impacts may not be problematic for all use cases, but performance testing should be considered as an integral part of the implementation strategy.

5.2.1. Implications for 3GPP PC5 and NG-PC5

Radio Access Layer (RAN) Considerations

PC5 sidelink is designed for direct communication between UEs (e.g. vehicle-to-vehicle). It has limited bandwidth and tight latency constraints. The introduction of PQC could:

- Increase packet sizes, leading to more frequent collisions or retransmissions.
- Require re-optimisation of scheduling and resource allocation to accommodate cryptographic payloads

Device Lifecycle and Upgradeability

Many V2X devices have long operational lifespans (10–15 years). Retrofitting PQC into these devices may not be feasible without:

- **Crypto-agility:** The ability to switch algorithms without hardware replacement.
- **Efficient firmware update mechanisms** to deploy PQC stacks securely
- Maturity and availability of relevant standards

5.2.2. V2X-Direct application taxonomy

The various applications using V2X-Direct communications for message delivery have different communications patterns, which will affect the impact of any move to post-quantum cryptography. This section of this document reviews the different communications patterns and assesses in a qualitative way the impact of moving to PQC for applications that follow this pattern. It is possible that for different types of application communications pattern, different approaches will need to be taken to mitigate the impact of that migration. This document does not specify or suggest those new approaches but merely provides the analysis of impact as background to future work which might study and suggest how PQC integration might happen for each pattern.

The application taxonomy used has not been formally published but has been informally discussed in other organizations and is proposed as a starting point for analysis. For each application type in the categorization, we provide a brief description and one or more examples of such applications from 5GAA USDPLOY, if applicable. Note that the taxonomy itself differs from the USDPLOY characterization, even though USDPLOY is used as the source of a list of applications.

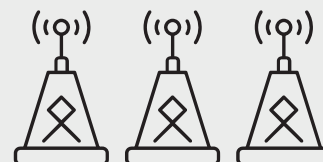
- Mobile Broadcast Simple:
 - These are messages that are sent by a mobile unit and for which there is no need to implement anti-tracking mechanisms. Since the units are mobile, (a) the instantaneous dynamic information about the unit changes rapidly and (b) they are in a dynamic communications environment, with the population of potential receivers of the message changing rapidly. As such the messages are sent frequently (multiple times per second) and must be authenticated such that a receiver can verify the authentication / sender authorization within a short time (convention is approximately one second) of encountering the sender (where “encountering” means “receiving a message from it for the first time”), and once the receiver has established the ability to authenticate the sender there are no further breaks in its ability to authenticate. Since the sender does not need anti-tracking, it can use the same certificate (or, more generically, credential) for a prolonged period.
 - USDPLOY examples: Basic Safety Message (BSM) when sent from emergency vehicle or school bus.



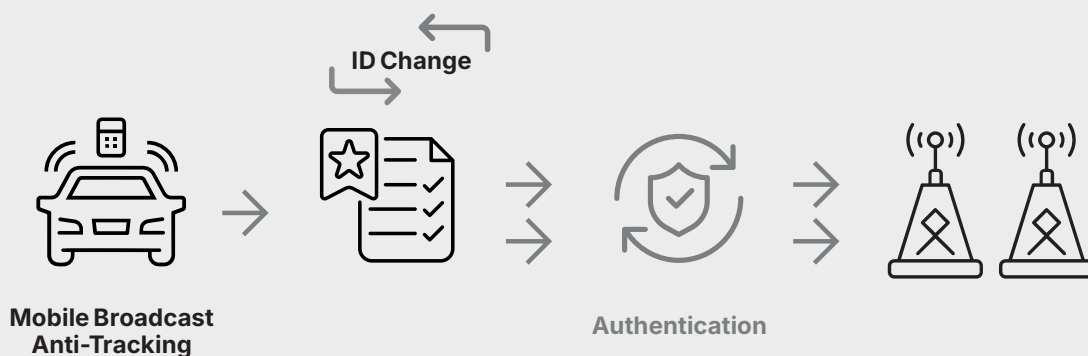
Mobile Broadcast Simple



Authentication



- Mobile Broadcast Anti-tracking
 - These messages have the same characteristics as the Mobile Broadcast Simple messages but include anti-tracking mechanisms. In particular, anti-tracking mechanisms can involve changing the signing certificate periodically, meaning that the security operations involve distributing new certificates from time to time. Apart from the certificate distribution feature, these applications behave like the Mobile Broadcast Simple applications. The preponderance of traffic over the V2X-Direct is expected to come from these applications because this class includes BSMs (which are frequent messages sent by vehicles, which will greatly outnumber infrastructure senders).
 - USDPLOY examples: Basic Safety Message (BSM)



- Mobile Unicast Non-Private
 - These messages are sent from a vehicle within the context of a communications session for a particular application. The sender may be sending to a single recipient or to a small number of recipients (so “Unicast” is an indicative rather than a normative name). Messages need to be authenticated but do not need to be encrypted, for example because they are intended for consumption by the primary receiver(s) but may contain information useful to other receivers for planning purposes. As such, they may be unicast at the application layer but will typically use broadcast mechanisms at lower layers. There are two different users of the authentication for these applications: the primary receiver(s) needs to be able to authenticate incoming messages very quickly after receiving them while other receivers may tolerate some delay before being able to authenticate the messages, or authentication may be less important overall for those receivers. This model is typically used when communication sessions are short, only a few exchanges, and so messages are individually secured rather than being secured within a session with an initial handshake. The sender may have anti-tracking requirements, in

which case it will change credential from time to time, or may have no anti-tracking requirements, in which case it can use the same credential for a prolonged period.

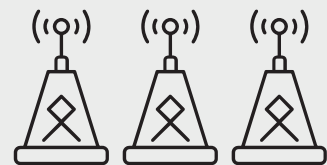
- USDPLOY examples: Signal Request Message (SRM). Other examples include Maneuver Coordination Message.



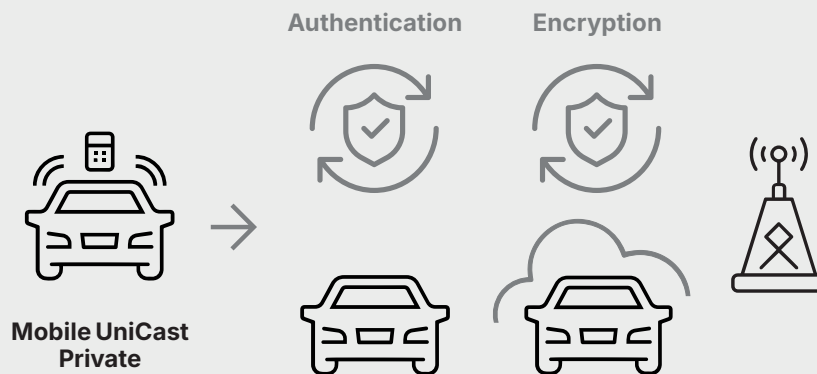
**Mobile UniCast
Non-Private**



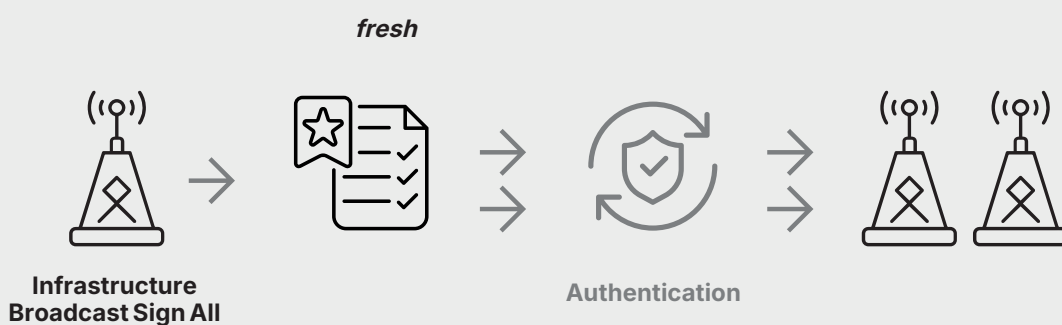
Authentication



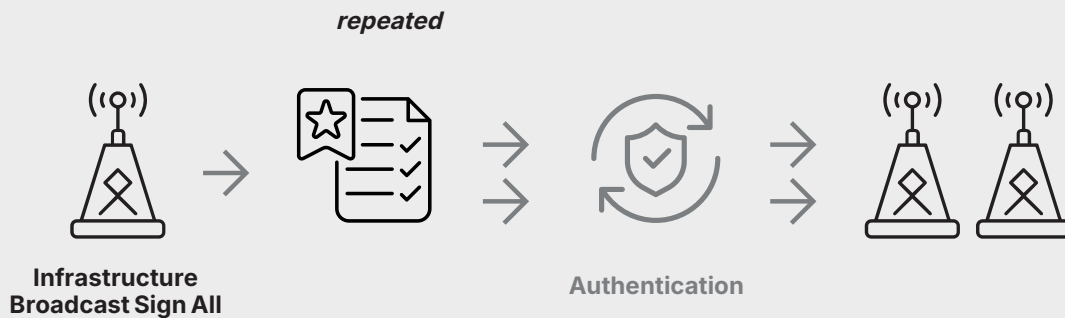
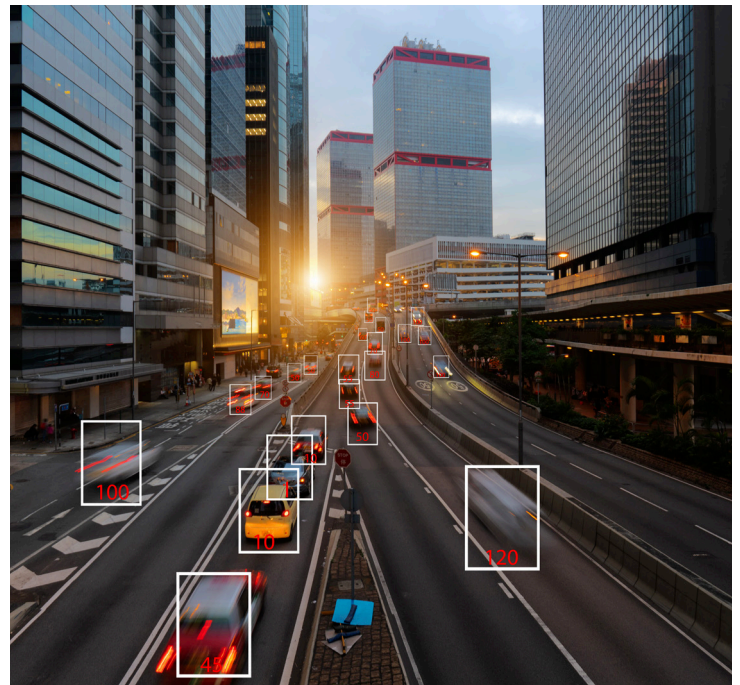
- Mobile Unicast Private
 - These messages are sent from a vehicle within the context of a communications session for a particular application. The sender may be sending to a single recipient or to a small number of recipients (so “Unicast” is an indicative rather than a normative name). Messages need to be authenticated and encrypted. They may be unicast at lower layers, or unicast at the application layer but broadcast mechanisms at lower layers. The receiver(s) needs to be able to authenticate incoming messages very quickly after receiving them. For short sessions, a natural model is to sign and public-key encrypt the message. For longer sessions, a natural model is to carry out some kind of handshake followed by symmetric authentication of messages. The ISO 21177 TLS model is intended to support longer sessions so this model is focused on one-shot encrypted response messages.
 - USDPLOY examples: Toll Usage Message per SAE J3217.



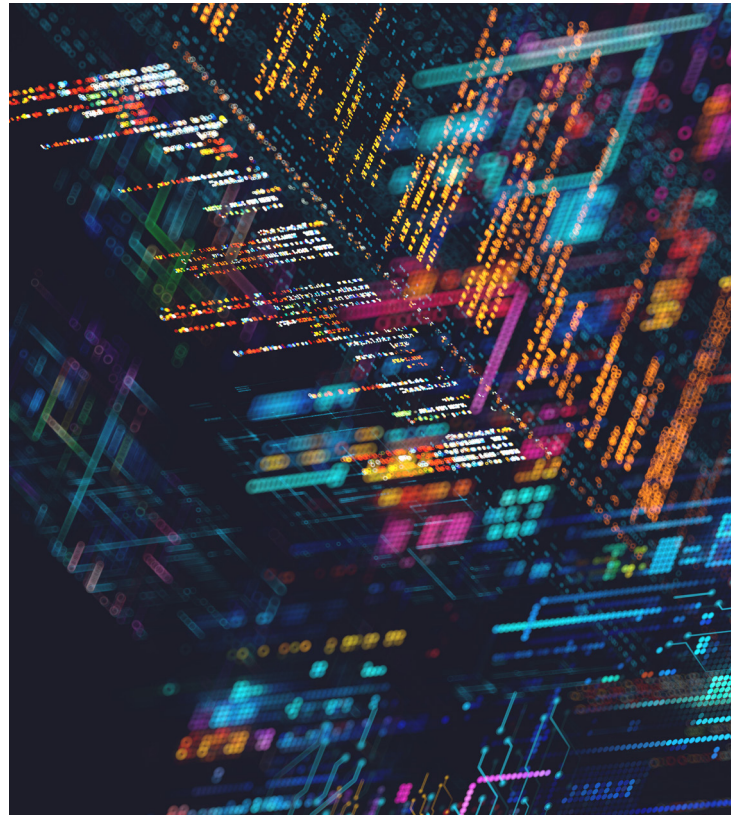
- Infrastructure Broadcast Sign All
 - These are messages that are sent by an infrastructure unit for which each instance of the message is (potentially) different and needs to be individually generated and authenticated. (The difference can be simply a different timestamp or include more significant differences about a state or status change for some system that is communicated about via the RSU). These messages are typically sent into a dynamic communications environment and so are sent frequently and must be authenticated such that a receiver can verify the authentication / authorization to send of the sender within a short time of encountering the sender, and once the receiver has established the ability to authenticate the sender there are no further breaks in its ability to authenticate. The sender can use the same certificate (or, more generically, credential) for a prolonged period.
 - USDPLOY examples: Signal Phase and Timing (SPaT), some uses of Traveler Information Message (TIM) and Road Safety Message (RSM)



- Infrastructure Broadcast Store and Repeat
 - These are messages that are sent by an infrastructure unit for which the information in the message changes infrequently, such that one instance of a message is frequently identical to the previous instance in terms of the information contained. As such, it is possible to generate (and sign or otherwise authenticate) the message once, store it, and rebroadcast it unchanged. These messages are typically sent into a dynamic communications environment and so are sent frequently and must be authenticated such that a receiver can verify the authentication / authorization to send of the sender within a short time of encountering the sender and whenever the message content changes. The sender can use the same certificate (or, more generically, credential) for a prolonged period.
 - USDPLOY examples: MAP, RTCM, some uses of Traveler Information Message (TIM) and Road Safety Message (RSM)



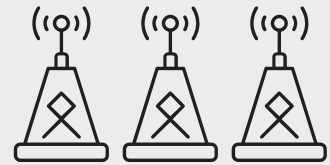
- Infrastructure Unicast Non-Private
 - These messages are sent from an infrastructure unit within the context of a communications session for a particular application. The sender may be sending to a single recipient or to a small number of recipients (so “Unicast” is an evocative rather than a normative name). Messages need to be authenticated but do not need to be encrypted, for example because they are intended for consumption by the primary receiver(s) but may contain information useful to other receivers for planning purposes. (As such, they may be unicast at the application layer but use broadcast mechanisms at lower layers). There are two different users of the authentication for these applications: the primary receiver(s) needs to be able to authenticate incoming messages very quickly after receiving them while other receivers may tolerate some delay before being able to authenticate the messages, or authentication may be less important overall for those receivers. A natural model has been to sign each message sent of this type but other models are possible.
 - USDPLOY examples: Signal Status Message (SSM); Toll Usage Message Acknowledgement (TUMAck – which is an example of a message which may be sent to multiple recipients)



**Mobile Unicast
Non-Private**



Authentication



- Infrastructure Unicast Private
 - These messages are sent from an infrastructure unit within the context of a communications session for a particular application. The sender may be sending to a single recipient or to a small number of recipients (so “Unicast” is an evocative rather than a normative name). Messages need to be authenticated and encrypted. They may be unicast at lower layers, or unicast at the application layer but broadcast mechanisms at lower layers. The receiver(s) needs to be able to authenticate incoming messages very quickly after receiving them. For short sessions, a natural model is to sign and public-key encrypt the message. For longer sessions, a natural model is to carry out some kind of handshake followed by symmetric authentication of messages. The ISO 21177 TLS model is intended to support longer sessions so this model is focused on one-shot encrypted response messages.
 - No USDPLOY examples
- ISO 2177 TLS
 - These messages are sent in the context of a TLS session where the handshake is carried out with 1609.2 certificates rather than X.509 certificates, as specified in ISO 21177 (which builds on IETF RFC 8902). They are unicast, and symmetrically encrypted and authenticated.
 - No USDPLOY examples.



5.2.3. Types of cryptographic overhead

The application types above incur cryptographic overhead in the following ways:

- **Authentication of application messages:** All messages need to be authenticated in a way that establishes the authorization of senders to send
- **Distribution of credentials:** sender credentials need to be provided to all receivers who might rely on them
- **Encryption:** In some cases, a public encryption key needs to be distributed and a response needs to be encrypted.

Summary

Message Type	Sender	Comms Mode	Authn	Encryption	Anti-tracking	Examples
Mobile Broadcast Simple	Mobile Unit	Broadcast	Yes	No	No	BSM (emergency vehicle, school bus)
Mobile Broadcast Anti-tracking	Mobile Unit	Broadcast	Yes	No	Yes	BSM
Mobile Unicast Non-Private	Mobile Unit	Unicast	Yes	No	Optional	SRM, Maneuver Coordination
Mobile Unicast Private	Mobile Unit	Unicast	Yes	Yes	Yes	Toll Usage Message (SAE J3217)
Infrastructure Broadcast Sign All	Infrastructure Unit	Broadcast	Yes	No	No	SPaT, TIM, RSM
Infrastructure Broadcast Store and Repeat	Infrastructure Unit	Broadcast	Yes	No	No	MAP, RTCM, TIM, RSM
Infrastructure Unicast Non-Private	Infrastructure Unit	Unicast	Yes	No	No	SSM, TUMAck
Infrastructure Unicast Private	Infrastructure Unit	Unicast	Yes	Yes	Yes	None
ISO 21177 TLS	Any	Unicast (TLS)	Yes	Yes (Symmetric)	Yes	None



5.2.4. Conclusions

The application taxonomy above provides some insight into requirements for PQC migration:

- Messages that use authentication incur overhead from signatures and certificates
- Messages that use encryption incur overhead from public-key encryption. They may carry out the public-key encryption once to establish a shared symmetric key, in which case the overhead of the encryption may be amortized over multiple messages, or they may carry out public-key encryption on individual messages, in which case each such message incurs public-key overhead
- Not captured in the above table is the frequency of the messages. Frequently sent signed messages cause more total overhead than infrequently sent periodic, or one-off, signed messages. It could be that a different approach is needed to securing frequently sent signed messages than the other messages, perhaps combining symmetric authentication with periodic public-key signatures.
- Also not captured in the above table is the concept of the impact of the messages: a message used for awareness is lower-impact than a message that requests signal pre-emption, for example. We suggest that analysis of the impact of the messages could inform the choice about what post-quantum security mechanisms to use.

5.3 Uu-based systems

This section examines the implications of PQC adoption for Uu-based systems, focusing on mobile telecommunications environments where cryptographic functions are deeply embedded in both signalling and application layers. Here

we analyse how quantum-safe strategies affect key aspects of Uu communications, including identity protection, network security protocols, and system performance, highlighting the tradeoffs between enhanced security and impacts on capacity, efficiency, and operational complexity in mobile networks. The primary task for the automotive industry here will be to engage with communication service providers (CSP) and supply chain partners to integrate emerging solutions into production systems to minimise on-road legacy and quantum vulnerability as part of an overall PQC transition.

5.3.1. PQC and mobile telecommunications

Communications executed through the Uu interface rely on public key cryptography at multiple points. Mobile Network Operators will need to bring their networks to quantum safe status by migrating currently deployed quantum-vulnerable cryptographic algorithms to post-quantum variants that offer protection against quantum-empowered adversaries. As an example, 5G mobile network connections currently rely on an identifier called a Subscription Permanent Identifier (SUPI). To avoid sending this identifier in the clear, an encrypted version called a Subscription Concealed Identifier (SUCI) is instead communicated between user equipment and the network. Concealment is achieved by using asymmetric cryptography to encrypt the SUPI, with the corresponding keys stored on the USIM. Current methods leverage a public key encryption scheme based on elliptic curve cryptography, which will be vulnerable to quantum attack. Hence, to achieve quantum safety it will be necessary to migrate these algorithms to quantum safe variants.

Not all cryptographic algorithms used for Uu communications are considered quantum vulnerable. As noted earlier, the nature of the quantum threat is quite different for symmetric algorithms, compared to

asymmetric algorithms, and some algorithms, such as the air interface confidentiality and integrity algorithms, and the authentication and key agreement algorithms (such as TUAK), are symmetric. Hence, not all algorithms involved in establishing/maintaining mobile network connections have a strong sensitivity to the quantum threat.

Hence, when connecting to the network, the SUCI will be quantum vulnerable, whereas the methods used to authenticate the user and establish a secure connection between UE and base station will be less impacted, owing to the underlying symmetric mechanisms. Beyond the base station, the standard set of mobile network security mechanisms are used, creating multiple known examples of potential quantum threats (see for example, this GSMA PQTN document). Examples that produce quantum vulnerabilities include asymmetric cryptography used in IPsec connections between base stations and security gateways, and in TLS connections used to secure data-in-transit between network components. These will need to be migrated to quantum safe mechanisms as part of operator migration efforts. For context, it is useful to distinguish two classes of traffic that traverse the Uu interface. First, as just discussed, there is signalling traffic between the UE and the mobile network itself — for example, procedures used to authenticate the subscriber and to establish a secure radio connection between the UE and the base station. These exchanges follow 3GPP-defined mechanisms such as EPS-AKA (LTE) or 5G-AKA (NR), which produce the keys used to secure the Uu air interface. Second, once the radio bearer is established, there is the application-layer

traffic associated with specific services — namely V2X communications. The security mechanisms used for these communications (e.g., authentication to a V2X application server, or end-to-end authentication between road users) are defined by the relevant V2X standards and may be entirely separate from 3GPP's subscriber authentication framework. The cryptographic mechanisms used for UE-network authentication via 3GPP methods generally differ from those used for securing V2X services. The latter depend on the specific V2X use case and typically involve distinct credentials, trust models, and key management schemes, so the question of quantum vulnerability must be analysed separately for both classes.



5.3.2. Impact of quantum-safe strategies on mobile network capacity & efficiency

The transition to quantum safety will involve implementing quantum-resistant cryptographic algorithms, known as Post-Quantum Cryptography (PQC), in mobile networks. These increase security but also come with trade-offs that can affect capacity and efficiency.

Efficiency Challenges

- **Increased computational load:** PQC algorithms can require more processing power than traditional RSA or ECC, especially for key generation and signature verification.
- **Larger key sizes:** Quantum-safe algorithms typically use longer keys and signatures, which can increase bandwidth usage and latency during authentication and encryption processes.
- **Energy consumption:** More complex cryptographic operations may lead to higher energy demands, especially in resource-constrained mobile devices and edge nodes.

Capacity Implications

- **Reduced throughput:** The overhead from larger cryptographic payloads can reduce the effective data throughput, particularly in dense network environments or during peak usage.
- **Spectrum efficiency:** If encryption-related signalling increases, it could marginally affect how efficiently spectrum is used for actual user data.
- **Infrastructure scaling:** Mobile network operators will need to ensure their infrastructure can handle quantum-safe protocols without bottlenecks.

Beyond capacity and efficiency, quantum-safe strategies can ripple across many layers of mobile networks and services.

Security Architecture & Protocol Design

- **Protocol Reengineering:** Existing protocols like TLS and IKEv2 encryption must be redesigned to accommodate post-quantum cryptographic primitives, which often have larger key sizes and different handshake flows.
- **Authentication Systems:** Subscriber identity protection (e.g. SUPI/SUCI) may shift from ECC to lattice-based schemes like ML-KEM, requiring updates to the authentication process and network-side verification systems.

Interoperability & Standards Compliance

- **Cross-Vendor Compatibility:** Ensuring seamless operation across diverse hardware and software ecosystems becomes more complex with PQC integration.
- **Roaming & Inter-PLMN Security:** Protocols like PRINS (Protecting Roaming using an Integrated Network Security solution - end-to-end application-level security enhancement over TLS) and SEPP (Security Edge Protection Proxy, gateway placed at the edge of home mobile networks to support security for roaming) must evolve to support quantum-safe encryption, impacting international roaming and inter-operator trust models.

Device & Firmware Management

- **Firmware Signing:** PQC algorithms like ML-DSA or SLH-DSA may replace ECC-based signatures, affecting how updates are signed, verified, and distributed.
- **Legacy Device Support:** Hybrid cryptographic models may be needed to maintain backward compatibility with older devices while introducing quantum-safe mechanisms.

6. Conclusions and next steps

Countries and agencies around the world are generally aligned on the need to migrate to Post-Quantum Cryptography (PQC). The common recommendation is to complete migration for high-priority systems by around 2030 and for all systems by approximately 2035, although dates may vary between geographies. Examples of government-issued PQC migration timelines can be found in [1–10]. Whether a system is high priority or not is determined by a variety of factors such as how long the data needs to remain confidentiality protected and what level of risk the data owner willing to bear. Some parts of telecommunications systems may be assessed by network operators to be of high priority. 5GAA is engaged with the European NIS2 Industry Collaboration Workstream to develop recommendations for the PQC transition that appropriately recognise the unique constraints of the automotive industry, including long-lived products and needs for interoperability with a significant deployed legacy base. Additionally, 5GAA is aware of ongoing activities focused on direct communications: ETSI TC ITS is working on an extension of the Threat, Vulnerability and Risk Analysis (TVRA) to include a cost-benefit analysis of mitigations to threats from quantum computers; the IEEE 1609 Working Group is starting the process to develop extensions to IEEE 1609.2 to support PQC algorithms and PQC-optimized protocols; and the Car-2-Car Communications Consortium is developing a white paper on the migration process.

Furthermore, it is important to note that the above timelines apply to deployments. For full PQC adoption in deployed systems, it is essential that standards are updated, and stable implementations are made available well in advance of those deployment milestones. The timelines for different stakeholders in the ecosystem, such as standards development organizations (SDO) and equipment vendors deploying the systems are inherently different. Standards bodies need to finalize specifications early, vendors need sufficient lead time to implement and only then wide-scale deployments can take place.

The automotive sector faces a challenge comparable to financial institutions transitioning to PQC: longlived products, distributed ecosystems, and safetycritical dependencies. To avoid exposing sensitive details and to align crossindustry expectations, a threestage riskassessment model is recommended:

Stage 1 - HighRisk / HighValue Targets

Systems where compromise would have material safety, operational, financial, or regulatory impact.

Action: Prioritise PQC readiness, cryptoagility, and migration feasibility analysis including mitigation options.

Stage 2 - ModerateRisk Assets

Systems where PQC effectiveness improves resilience but immediate migration may be constrained by lifecycle or performance factors.

Action: Apply “besteffort PQC transition,” mitigations, and monitoring.

Stage 3 - LowRisk or Currently NonMigratable Assets

Systems with minimal exposure, no feasible migration path, or long-term phasing-out.

Action: Document risk acceptance, maintain compensating controls, and revisit periodically.

7. References

1. NIST IR 8547: "Transition to Post-Quantum Cryptography Standards".
2. EU, Roadmap for the Transition to Post-Quantum Cryptography
<https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography>
3. UK NCSC, Timelines for migration to post-quantum cryptography
<https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>
4. NSA, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ
https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
5. ANSSI, Guide des Mécanismes cryptographiques
https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf
6. ASD, Guidelines for cryptography
<https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography>
7. Canadian Centre for Cyber Security, Roadmap for the migration to post-quantum cryptography
<https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001>
8. Swedish NCSC, Kvantsäker kryptografi
<https://www.ncsc.se/sv/aktuellt/kvantsaker-kryptografi/>
9. NSM Cryptographic Recommendations
<https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf>
10. AIVD, The PQC Migration Handbook
<https://english.aivd.nl/binaries/aivd-en/documenten/publications/2024/12/3/the-pqc-migration-handbook/The+PQC+Migration+Handbook+.pdf>

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
UK

www.gsma.com
Email: info@gsma.com

GSMA

5GAA c/o MCI Munich
Lindwurmstraße 25,
80337 München,
Germany

www.5gaa.org
Email: liaison@5gaa.org

