Institution: Royal Holloway, University of London

Unit of Assessment: 12 Engineering

Title of case study: Standardisation of the TUAK Algorithm for eSIMs: Transforming Security for Internet of Things and Consumer Devices Worldwide

Period when the underpinning research was undertaken: 2014-2018

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Keith Mayes	Professor of Information Security	2002-date

Period when the claimed impact occurred: 2017-2020

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact

Engineering research undertaken by Professor Keith Mayes, at the request of the European Telecommunications Standards Institute (ETSI), proved the feasibility of securely implementing the TUAK algorithm in eSIM devices. This removed a security risk that had been a barrier to widespread eSIM adoption in mobile communications networks. His research has supported market growth in areas including, consumer devices, automotive, smart manufacturing (Industry 4.0), smart metering, and is influencing plans for remote healthcare. Between the start of 2017 and the end of 2020, a total of approximately 1,398,000,000 eSIMs were issued, with approximately 622,000,000 of them in consumer devices. At the end of 2020 over 20 flagship smartphones supported eSIM technology.

2. Underpinning research

To support cellular communications in the Internet of Things (IoT), an embedded Subscriber Identity Module (SIM) chip was needed that could be remotely and securely provisioned/re-provisioned to provide authenticated access to different mobile networks. The solution was standardised, becoming the embedded SIM (eSIM), also fitted in mainstream Smartphones and personal devices. Remote eSIM Service Provisioning (RSP), requires a common authentication and key establishment algorithm that can be reconfigured, rather than replaced when changing networks. Mobile networks had one de-facto common standard algorithm called MILENAGE. However, as eSIMs will be in billions of things, it was an unacceptable security risk for the telecommunications industry, to have eSIM and RSP reliant on a single algorithm; in case a security vulnerability emerged. Therefore, to make eSIM and RSP feasible, it was necessary to develop a second algorithm based on a completely different design (called TUAK); so both are unlikely to share common security vulnerabilities. The responsibility for this, fell to the Security Algorithm Group of Experts (SAGE) of the European Telecommunications Standards Institute (ETSI), who tasked Mayes with the first ever evaluation of the practicality of secure implementation within deployed and/or new eSIM chips. The Mayes work received some funding contribution from government (GCHQ) and the GSM Association (GSMA); specialist tools were provided by MULTOS and Crisp Telecom.

Mayes was a credible choice for the research, having previously contributed to related ETSI and Third Generation Partnership Project (3GPP) international telecommunications standards while working in industry; and for subsequently founding (in 2002) the Smart Card Centre (SCC) at Royal Holloway University of London, with telecommunications industry funding. SCC engineering research (hardware and software) includes implementation and evaluation of security algorithms on specialist attack-resistant microcontroller chips e.g. in conventional SIMs, phones and IoT devices; including security testing at native (chip-level) and platform-level. The

latter characterised by high security evaluation, but much slower speed than native implementation; unless crypto-coprocessor hardware is added to accelerate algorithms.

Mayes research within the SCC, in support of ETSI, initially created baseline implementations of the new common authentication algorithm, TUAK, on two advanced security chips and two MULTOS platforms using those chips; subsequently, a legacy chip was evaluated. A server baseline was also created (supported by Ericsson), representing the network Authentication Centre. Implementation strategies were refined over multiple iterations, identifying and optimising pre-computations to the extent permitted by very limited memories and using hardware features accessible at chip or platform level. Equipment included sample chips and platforms (MULTOS), software development and test environments; digital oscilloscopes, a power-leakage test rig and a legacy chip hardware emulator from Crisp Telecom.

The main research findings of Mayes, captured in standards reports and academic publication, were:

1) It was feasible to implement the algorithm at chip-level, with adequate performance, even on 16-bit legacy security chips without the need for hardware crypto-coprocessors.
2) It was not advisable to download the algorithm at the platform-level of deployed SIMs, as the speed was too slow and some side-channel power leakage (potential to infer sensitive data from power consumption variations) was detectable.

Finding (1) proved to ETSI and 3GPP that the algorithm was feasible on both new and legacy SIM chips; and as a result, 3GPP added the TUAK algorithm (and Mayes reports) to its international standards. In parallel, the GSMA was standardising the Remote eSIM Provisioning specifications and responded to finding (1) by accepting TUAK as a suitable security algorithm, and to finding (2) by mandating both MILENAGE and TUAK support within all eSIMs. Publication of the GSMA specification (December 2016) very notably accelerated the rollout of eSIMs; with approximately 1,398,000,000 deployed by the end of 2020.

3. References to the research

The Mayes TUAK research evidence is found in technical reports for ETSI and GSMA, within 3GPP international standards and within related peer-reviewed academic publications. Quality is determined, by global international standards bodies commissioning the research and then accepting and publishing the results, by the endorsement letters of leading industry experts directly involved in this work, by the engagement of industry expert authors within peer-reviewed accepted conference publication, and by being one of the papers invited to publish an extended version in a related journal. The work began February 2014 helped by GCHQ's competitive small grant scheme (GBP25,000), Mayes PI. It was extended in October 2014 helped by private funding from the GSMA (EUR5,000), Mayes PI.

It is emphasised that the 3GPP 35.935 international telecommunications standards document exists, *solely* to refer to the Mayes research findings, via the ETSI technical reports listed below.

[R1] TR 35.935 Specification, version V13.0.0 (2016-01) onwards, of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Performance Evaluation https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2409.
[R2] "Performance Evaluation of the TUAK algorithm in support of the ETSI Sage standardisation group"; Keith Mayes; ISG Smart Card Centre, Royal Holloway University of London. Available from HEI on Request.
[R3] "Performance Evaluation of the TUAK algorithm in support of the GSMA and ETSI SAGE standardisation group"; Keith Mayes; ISG Smart Card Centre, Royal Holloway University of London. Available from HEI on Request.

There is an ETSI equivalent/reference to the 3GPP TR 35.935 document.

[R4] ETSI TR 135 935 V13.0.0 (2016-01) Universal Mobile Telecommunications System (UMTS); LTE; Performance evaluation of the Tuak algorithm set https://www.etsi.org/deliver/etsi_tr/135900_135999/135935/12.00.00_60/tr_135935v120000p.pdf

Academic Conference Paper
[R5] K. Mayes, S. Babbage, and A. Maximov, "Performance Evaluation of the new TUAK Mobile Authentication Algorithm," in Proc. ICONS/EMBEDDED, pp. 38-44, 2016.
Extended Journal
Paper http://www.thinkmind.org/index.php?view=article&articleid=icons_2016_3_10_47006
[R6] K. Mayes, S. Babbage, and A. Maximov, "Multi-Platform Performance Evaluation of the TUAK Mobile Authentication Algorithm", International Journal On Advances in Security, pp158-168 2016 no 3&4, articleid:
55009 http://www.thinkmind.org/index.php?view=article&articleid=sec_v9_n34_2016_7.

4. Details of the impact

Cellular connectivity of machines, and personal devices, is key to realising the Internet of Things (IoT). Removable SIM cards have become impractical from environmental, operational and manufacturing viewpoints, and need to be replaced by embedded SIMs (eSIM).The mass deployment of eSIMs with reliance on just the 3GPP MILENAGE algorithm was considered too great a risk by the telecommunications industry. Mayes research, undertaken on behalf of ETSI, for the standardisation of the TUAK algorithm, mitigated this risk and was a pivotal enabler for eSIM roll-out.

Transforming industry capability by producing globally accepted standards for eSIM

The engineering research Mayes undertook was critical to TUAK and eSIM standardisation, as evident from current ETSI and 3GPP standards [R1] and the opinion of the Vodafone [text removed for publication], who is also [text removed for publication] ETSI Security Algorithms Group of Experts (SAGE); the design authority for TUAK standardisation [S1].

"[text removed for publication]." [S1].

Prior to 2017, non-standard eSIMs had failed to achieve significant growth. The critical change was publication of version 2.0 of the GSMA RSP eSIM standards, which mandated TUAK, (an earlier version had only limited take-up for smartwatches). This was summarised by the eSIM [text removed for publication] for the GSMA.

"[text removed for publication]." [S2].

Transforming global markets with eSIM

Following standardisation, deployment of eSIMs in consumer devices rapidly accelerated as illustrated in Figure 1; representing the number of eSIMs issued per year. By December 2020 approximately 622,000,000 had been deployed in total; and more than 20 flagship Smartphones (Apple, Samsung, Google and Huawei) plus tablets and PDAs, supported eSIM [S5].

(millions)

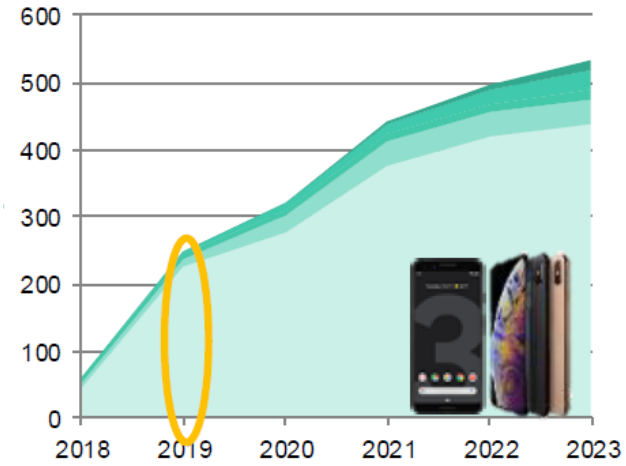

Figure 1 Deployed Consumer eSIMs [S4] [S3]

(billions)

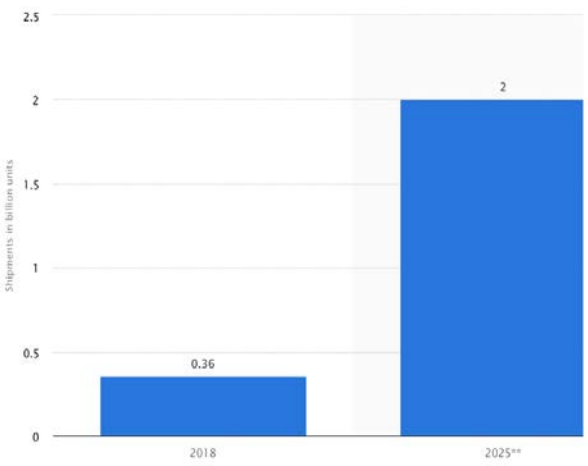

Figure 2 Annual Global Shipments of eSIMs

Figure 2 indicates the number of eSIMs issued per year for all uses (consumer and non-consumer) [S3]. Based on the published data, 360,000,000 were shipped in 2018 and using the market report's [S3] calculation of 27% CAGR, an approximate total of 1,398,000,000 eSIMs had been issued by the end of 2020, predicted to be rising at a rate of 2,000,000,000 per year by 2025. At the end of 2020, approximately 776,000,000 of deployed eSIMs were for a mix of automotive, industrial and other IoT uses.

Beneficiaries of secure eSIM are diverse and on enormous scale. Manufacturers of eSIM chips, are now producing standardised, rather than network-specific eSIMs. Mobile and IoT manufacturers can produce devices that are smaller, more robust and tolerant to extreme environments. Mobile network operators can offer connectivity via a range of devices, without SIM card deployment costs. Billions of end-users benefit by simple connection and reconnection of consumer devices to preferred networks. Two existing and major market sectors are now presented.

Automotive/connected-cars is an exciting market (estimated worth in 2020 USD151,800,000,000), critically enabled by eSIM, as reported by GSMA and Ericsson [S6, S7]. Vehicles must withstand extremes of operating environment, yet remain reliable and secure for decades, with increasing reliance on cellular communications.

"eSIM: Driving global connectivity in the automotive industry… all cars built will be cellular-enabled, leading to an enhanced driving experience made possible by innovative connected services, like assisted driving and better infotainment." [S7].

The eSIMs are installed into vehicles at manufacture, however, at that stage it is impossible to predict all owners, networks or countries that will span the vehicle life.

"From a connected vehicle's birth in the factory, to the port, to dealer, to the consumer – no matter where in the world it goes -- eSIM allows for a steady, compliant, high performant local connection, and most important, seamless." [S7].

"...GSMA's Embedded SIM Specification uses Remote SIM Provisioning technology and therefore enables late stage programming of M2M devices. In the auto sector, this will massively simplify production and will accelerate the growth of the connected car market..." [S6].

The Industrial IoT Market was worth USD126,000,000,000 in 2019, and with CAGR of 29.4%, is predicted to have reached USD163,044,000,000 by end of 2020; aided by eSIM technology

[S8]. The Ericsson whitepaper on *"The cellular connected enterprise – from products to production"* [S8], explains the importance of cellular communications in industrial IoT and how eSIM simplifies integration, unlocking value across the market.

"…To leverage supply chains and multiple factories across the globe … enterprises receive simplified global connectivity management by exploiting eSIM capabilities for seamless device deployment…Key benefits of global IoT Connectivity… (1) Faster time to market, build and scaling global cellular IoT efforts faster, (2) Reduced integration costs, (3) Future proof products, (4) Improved cost savings by tracking and controlling assets remotely, (5) Simplified, more integrated supply chain, (6), Increased security" [S8].

The opinion of the Thales Marketing Director for Embedded Products, further emphasises the strong linkage between eSIM and IoT market development.

*"…*the standardisation of the TUAK security algorithm, by the European Telecommunications Institute (ETSI) and the Third Generation Partnership Project (3GPP); and *standardisation of the embedded SIM (eSIM) by the GSM Association (GSMA), have represented a major achievement to enable the mass roll-out and business potential for mobile connected devices within the Internet of Things (IoT). It is the combination of security … and remote provisioning capability … that makes the eSIM so suited to a range of our markets…" [S9].*

A further market to consider is the **Medical IoT Market**, which considering several market reports [S10], had a value in 2019 of between USD57,620,000,000 and USD113,750,000,000. Current medical IoT solutions include, chronic care, assisted living, remote treatment, sleep therapy, blood sugar and pressure meters, and cardiac monitors.

"IoT healthcare solutions have the potential to dramatically improve patient outcomes and save millions of lives with remote patient monitoring..." [S10].

eSIMs are not yet deployed in significant numbers within this market, but their properties of security, support for data privacy, reconfiguration, and environmental tolerance, are positively impacting manufacturer design strategy for connected medical devices. This is particularly important, as the majority of health care organisations that have so far deployed medical IoT devices have experienced cyberattacks against their legacy technologies [S10].

5. Sources to corroborate the impact

Corroboration of the linkage and impact to telecommunications standards and to eSIM requirements and roll-out; numbered supporting documents.

S1) Testimonial letter from the Vodafone [text removed for publication] of ETSI SAGE.
S2) Testimonial letter from the former eSIM [text removed for publication] for the GSMA.
S3) Summary of Statista data (2020) on eSIM shipments per year.
S4) Slides from Google/G&D/EE, emphasising importance of eSIM and forecasting consumer device (e.g. smartphones) eSIM market growth.
S5) eSIM supported consumer devices as of November 2020.
S6) GSMA report on how eSIM is transforming the connected car market.
S7) Ericsson blog: "eSIM: Driving global connectivity in the automotive industry". Illustrates the importance and value of eSIM to automotive related industries.
S8) Industrial IoT market information and Ericsson whitepaper.
S9) Testimonial letter from the Thales Marketing Director for Embedded Products.
S10) Medical IoT market information.