Monero Distribution Company (Pty) Ltd

Software Security Assessment Services

RandomX Source Code Audit

April 12, 2019
Version: 1.0

Presented by:

Ryan Spanier, Head of Solution Architecture and Research

Nagravision S.A. – Kudelski Security
Route de Genève 22-24
CH-1033 Cheseaux-sur-Lausanne
Switzerland

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Monero (XMR) is an open-source cryptocurrency created in April 2014 that focuses on privacy and decentralization that runs on Windows, macOS, Linux, Android, and FreeBSD. Monero uses a public ledger to record transactions while new units are created through a process called mining. Monero aims to improve on existing cryptocurrency design by obscuring sender, recipient and amount of every transaction made as well as making the mining process more egalitarian.

RandomX is a proof-of-work (PoW) algorithm, developed by Monero, that is optimized for general-purpose CPUs. RandomX uses random code execution together with several memory-hard techniques to achieve the following goals:

- Prevent the development of a single-chip ASIC
- Minimize the efficiency advantage of specialized hardware compared to a general-purpose CPU

Monero Research Lab would like a third-party review of the source code of their new RandomX PoW algorithm. The audit will be crowdfunded by their community and Monero would thus like to publish the results of this audit.

Following discussions with Howard Chu, Monero Distribution Company (Pty) Ltd, and JP Aumasson, VP Techology, Kudelski Security, an offer for a comprehensive security audit of the RandomX PoW code was requested. Kudelski Security would like to thank Monero for the opportunity to present our offer for this security assessment.

Engagement Objectives

In coordination with Monero Distribution Company (Pty) Ltd, Kudelski Security has identified the following engagement objectives:

- Help Monero Management, users, and developers to better understand the current risks and security postures of their code base.
- Provide a professional opinion on the maturity, adequacy and efficiency of the security measures that are in place within the RandomX proof-of-work (PoW) algorithm.
- Identify potential issues and include improvement recommendations based on the result of our review.
- Propose prioritized improvements and recommendations to mitigate identified risks and vulnerabilities.

Activities

- Security audit of RandomX source code focusing on critical cryptographic components, with a goal of finding security defects, misue of cryptographic components and APIs, unsafe coding risks, and matching the intended behavior as documented in the specifications.
- Security audit of the design and protocol as specified in doc/*md files.
- Propose improvements in terms of parameter choices and source doce optimization targets, if applicable.
- Provide remediation recommendations and perform re-testing.

Key Points

- The engagement will be conducted by Yolan Romailler, Cryptography and Research Engineer, Dr. Tommaso Gagliardoni, Cryptography and Research Engineer, and Dr. Jean-Philippe Aumasson, VP Technology.
- This engagement is estimated to be completed over a period of three (3) weeks with a firmed fixed price of CHF 18,250. See below for a description of services:
  - Research, Cryptography, & Security Engineering Services – CHF 17,500
  - Project Management Services – CHF 750

  Kudelski applied a special rate for engineering services (discounted 15%), which represents our strong desire to work with you on this prestigious project.
- All work will be delivered remotely.
- For all cryptography engagements, additional workload can be divided into 5 (five) day work packages.

Engagement Deliverables

- Technical report detailing findings, with executive summary and a remediation plan composed of actionable recommendations.
- Presentation of findings with Monero internal stakeholders.

Engagement Location

The engagement will be executed remotely.

ENGAGEMENT SCOPE AND ACTIVITIES

Engagement Preparation

Prior to the start of the engagement, Kudelski Security will host and lead a kickoff call with the Monero Distribution Company (Pty) Ltd sponsor and designated point of contact to gather detailed information necessary to ensure a successful engagement.

The primary goals of this kickoff meeting are to:

- Finalize the scope and timelines for the engagement’s commencement and duration.
- Validate that goals and scope are accurately captured in the Statement of Work.
- Ensure activities are understood and coordinated prior to commencement.
- Identify any obstacles or challenges to completion that may be unique to Monero Distribution Company (Pty) Ltd.
- Identify key stakeholders from both Kudelski Security and Monero Distribution Company (Pty) Ltd who need to be included in the engagement updates and escalations.
- Agree on secure communication path.

Engagement Description

The intent of the Software Security Assessment is to evaluate the security level of the Monero RandomX algorithm and code base, and to propose adequate mitigations to the issues identified.

This assessment will answer the following questions:

- How safe are the cryptographic algorithms and protocols used in the software?
- How safe are the implementations of said cryptographic components?
- Can the product or protocols or their implementations be abused by attackers?
- Does the RandomX PoW implementation work as intended?

It will include the following activities:

- Review of the source code
- Implementation of proof-of-concept attacks, for any vulnerability identified

The outcome will be provided in the form of a detailed report and remote presentation, including relevant data and recommendations to guide the prioritized remediation. Kudelski Security will provide a final version for a public report. The publication of the report shall be done by Monero with at least 3 days prior notice to Kudelski Security.

Detailed Scope

The detailed scope below is based on your project, described in the executive summary. From your discussions with Dr. Jean-Phillipe Aumasson, we estimate that we can complete the audit over a period of three (3) weeks.

Detailed Scope

Preparation, Exploration, Documentation

Tasks:

- Grasp the codebase and review RandomX documentation.
- Define test strategy.
- Prepare environment.
- Finalize Statement of Work (SoW) and hold the kick-off meeting.

Deliverables:

- Statement of Work (SoW).

Code Review and Reporting

Tasks:

- Review selected portions of the source code provided
- Security review of the design and protocol as specified in documentation.
- Recommendations to fix identified vulnerabilities.

Deliverables:

- Technical report describing issues identified and mitigation recommendations
- Informal description of any critical issue prior to the report delivery

Final Client Audit Report and Presentation

Tasks:

- Summarize discovery, structured attack scenarios and results.
- Present and explain the suggested recommendations.
- Update the document to include Monero’s responses to findings.
- Provide expert opinion on the effectiveness of Monero’s mitigations.

Deliverables:

- Updated technical report with detailed findings, executive summary and a remediation plan composed by actionable recommendations.

ENGAGEMENT DELIVERABLES

The outcome will be provided in the form of a detailed report and remote presentation, including relevant data and recommendations to guide the prioritized remediation.

Kudelski Security will provide Monero Distribution Company (Pty) Ltd with the following deliverables in electronic format:

- **Executive Summary Presentation** designed for Senior Leadership Team / CISO (PDF).
- **Engagement Findings and Technical Report** designed for Managers and Program Owners.

Kudelski Security will deliver the Executive Summary presentation to Monero stakeholders per agreed timeline, and via client instruction.

Deliverable Acceptance

All deliverables defined in this offer are subject to inspection and acceptance by the Monero Distribution Company (Pty) Ltd Designated Contact.

Kudelski will provide for one (1) round of draft review, during which Monero Distribution Company (Pty) Ltd will be given an opportunity to review and comment to ensure a deliverable is complete and accurate and that it meets expectations. Kudelski Security will provide the finalized deliverable for Monero Distribution Company (Pty) Ltd acceptance or rejection. If the deliverable does not conform to the agreed-upon acceptance requirements, Monero Distribution Company (Pty) Ltd shall notify Kudelski Security in writing, setting forth Monero Distribution Company (Pty) Ltd rejection and the basis of the nonconformity. Kudelski Security shall correct such nonconformity within a mutually agreeable timeframe.

Monero Distribution Company (Pty) Ltd will accept or reject the deliverable(s) within five (5) business days of completing each iteration. If Monero Distribution Company (Pty) Ltd does not accept or reject the deliverable(s) within this period, the deliverable(s) shall be considered accepted by Monero Distribution Company (Pty) Ltd.

Scheduling

Kudelski cannot schedule services or determine detailed engagement timelines until the SOW is mutually executed. Following SOW signature, Kudelski Project Management Office (PMO) will contact Monero Distribution Company (Pty) Ltd’s Designated Engagement Manager (DEM) to establish engagement start dates based on then-current scheduling factors for both parties. Kudelski is committed to providing an appropriate consulting resource within a timeframe that is agreed upon with Monero Distribution Company (Pty) Ltd during the engagement kickoff meeting. However, engagement start and/or end dates cannot be guaranteed, as many factors outside of Kudelski control can alter engagement timelines.

Rescheduling or Cancellation

Two (2) weeks’ written notice in advance of cancelling or rescheduling the consultant resource is requested. Notices can be sent via email to the Kudelski Security project manager.

ENGAGEMENT RESPONSIBILITIES

Kudelski Security Responsibilities

Kudelski will:

- Directly manage Kudelski Consultants and Project Managers, excluding any Monero Distribution Company (Pty) Ltd contracted consultants or third parties, unless agreed to in writing.
- Follow all reasonably written security rules and procedures provided by Monero Distribution Company (Pty) Ltd.
- Serve as the primary point of contact for the life of the engagement.
- Facilitate the engagement kick-off meeting.
- Manage the engagement budget and Change Order process (if needed).
- Coordinate Kudelski personnel logistics.

- Prepare and deliver status reports on regular intervals as determined by Monero Distribution Company (Pty) Ltd's DEM.
- Ensure deliverables meet the Monero Distribution Company (Pty) Ltd sponsor's approval within the boundaries of the scope of the engagement.
- Ensure engagement work is completed as agreed upon in the SOW and obtain Monero Distribution Company (Pty) Ltd sign-off.

Monero Distribution Company (Pty) Ltd Responsibilities

Monero Distribution Company (Pty) Ltd will:

- Designate one employee to serve as a primary DEM for the engagement. The DEM will serve as the as the first point of escalation for any engagement-related requests or issues, and
- Provide access with necessary consents, permissions, and authorizations to all proprietary information, hardware and software applications, and other systems necessary, whether owned, leased, or licensed, before starting services and until services are completed,
- Execute all data gathering activities in an efficient manner, and data will be promptly submitted to Kudelski resources within a commercially reasonable response time,
- Abide by Standard Operational Procedures, applicable regulations, manuals, texts, briefs and other materials associated with the engagement and the hardware/software noted throughout this SOW,
- Provide the necessary staff availability to complete identified tasks and/or to participate in interviews to ensure the agreed-upon completion dates, tasks or deliverables,
- Provide access to any necessary facility and/or remote access to complete the engagement during normal business hours or other agreed times.

KEY PERSONNEL

NAME	FUNCTION	PHONE	EMAIL
Monero Distribution Company (Pty) Ltd CONTACTS			
Howard Chu			
KUDELSKI SECURITY CONTACTS			
Ryan Spanier	Head of Solution Architecture and Research		
JP Aumasson	VP Technology		

ENGAGEMENT PRICING

Financial Terms

Kudelski will invoice Monero Distribution Company (Pty) Ltd for the total amount listed in the table below as a fixed engagement fee. Please note this engagement is not billed as time and material.

DESCRIPTION	TOTAL
Research, Cryptography, Security Engineering Services	**CHF 17,500**
Project Management Services	**CHF 750**
TOTAL	**CHF 18,250**

- Please note that if the workload increases for this or any other engagement for Monero Distribution Company (Pty) Ltd beyond 30 days, volume discounts will apply.
- Invoice will be sent at the end of the engagement once the final deliverable is accepted.
- Should Monero Distribution Company (Pty) Ltd require additional resources or complementary skill sets, Kudelski Security will submit separate commercial offers for approval and apply the same volume discounts, if applicable.

General Conditions

All engagement orders under this service proposal shall be subject to the “Terms & Conditions of the offer – Security Assessment Services” attached hereto. In case of conflict between the “Terms & Conditions of the offer – Security Assessment Services” and this offer, the terms of this offer shall prevail.

- The resources will be under the responsibility and direct management of Kudelski Security Project Managers.
- Travel and accommodation will be invoiced at cost and separately with justification elements.
- Kudelski Security will respect client travel and accommodation policies for the expenses incurred over the course of the engagement.
- Invoices will be delivered monthly.
- Terms are net 30 days.
- Any additional services proposed during the engagement will be subject to a separated commercial offer and to Monero Distribution Company (Pty) Ltd approval before proceeding.
- Upon request, Kudelski Security will delete all assessment data on its network after final client sign-off. This will be confirmed by e-mail confirmation to client.
- A bilateral non-disclosure agreement will be agreed and signed by both parties prior to initiating the project.

EXECUTION OF SOW

This SOW is governed by the General Terms and Conditions in the Appendix and effective on the date of last signature below. By signing, you accept those Terms and Conditions. Upon signature, email to KSEMEASalesOperations@nagra.com. If submitted via DocuSign, the SOW will route automatically. If this SOW is not signed within 30 days of the publish date, all services, terms, and prices herein are subject to change and/or rescoping.

Nagravision S.A.	**Monero Distribution Company (Pty) Ltd**
Authorized Signature	Authorized Signature
Name (Print)	Name (Print)
Title	Title
Date	Date

APPENDIX: GENERAL TERMS AND CONDITIONS

1. Agreement. The scope of services, additional terms in this engagement or statement of work, these General Terms and Conditions, the annexes, attachments, and exhibits (change order and certificate of completion and acceptance) are collectively referred to as the "SOW". This SOW forms the entire agreement between the Client and Kudelski Security and supersedes and replaces any previous communications, representations or agreement, electronic, written or oral. In the event of a conflict between the terms in the SOW and these General Terms and Conditions, then the terms of the SOW control. The sale of or an order to perform any services is expressly conditioned on Client's assent to the terms of this SOW. Any other additional or inconsistent terms or conditions, including warranties or indemnities, in a purchase order, authorization to proceed, or other document or communication from the Client or course of dealings between the parties or usage of trade are expressly disclaimed and rejected.

2. Payment. Unless expressly listed in the SOW, invoices are due thirty (30) calendar days from the date of the invoice without any set-off, offset or deduction of any payment not due, taxes or otherwise in the currency indicated on the invoice. Kudelski Security may invoice Client for installment of services. Kudelski Security reserves the right to suspend Services until payment is received. Client agrees to pay interest on all past-due sums at the lower of 1.5% per month or the highest rate allowed by law.

3. Term and Termination. This SOW begins on the date of last signature and ends upon completion of the services. Either Party may terminate this SOW before completion with 30 calendar day's written notice to the other Party. Termination does not relieve Client's obligation to pay for services rendered and costs incurred by Kudelski Security. Kudelski Security may suspend or terminate this SOW, or any portion of it, immediately for cause if Client becomes insolvent, bankrupt, materially breaches the terms of this SOW, including failure or delay in payment of invoices.

4. Client Data and Kudelski Security Intellectual Property.

4.1 Client Data. Client owns all right, title and interest in any data provided by Client to Kudelski Security or made available to Kudelski Security through Client systems ("Client Data") in the performance of Services. Client grants Kudelski Security for the Term of this SOW a limited, non-exclusive, revocable license to use the foregoing Client Data solely for performing the Services under this SOW.

4.2 Kudelski Security Intellectual Property. Excluding Client Data, Kudelski Security retains all right, title and interest in any pre-existing intellectual property, any modifications or improvements to the pre-existing intellectual property, and any deliverable or assessment specifically created or developed by Kudelski Security for Client in the performance of Services (collectively, Kudelski Security Property). Subject to Client's full payment of applicable invoices, Kudelski Security grants Client and any Affiliated Company (defined below) of Client a worldwide, non-exclusive, royalty-free, perpetual, fully paid, irrevocable license: (a) to modify any Kudelski Security Property to create a derivative work of Kudelski Security Property (Derivative Work); (b) to reproduce the Derivative Work of the Kudelski Security Property; (c) to distribute the Derivative Work of the Kudelski Security Property, but only to an Affiliated Company of Client; and (d) to use any Kudelski Security Property or any Derivative Work for Client's own internal business purposes. For purposes of this Section 4.2, "Affiliated Company" means any legal entity that Client controls, that controls Client, or that Client is under common control at the Effective Date of this SOW and for so long as such control exists. Control is defined as exercising 50% or more of the voting rights.

4.3 Follow-On Licensing. Following the completion of the Services in this SOW and the subsequent delivery of the deliverable or assessment to Client, should the opportunity arise for licensing of any Kudelski Security Intellectual Property, the parties will mutually agree on a definitive license agreement separate and distinct from this SOW as to any licensing of Kudelski Security Intellectual Property.

5. Warranties, Remedies, and Disclaimers. Kudelski Security warrants that the services and any deliverable created from the services will be performed: (a) in a workmanlike and professional manner consistent with generally accepted industry standards, and (b) substantially conform to the written specifications of the SOW for 30 calendar days from completion. Client's sole and exclusive remedy and Kudelski Security's entire liability with respect to this services warranty will be, at Kudelski Security's option and expense, to either use its reasonable commercial efforts to re-perform any non-conforming services not in substantial compliance with the warranty in this SOW or refund amounts paid by Client related to the portion of the services not in substantial compliance. In each situation, re-perform or refund, Client must notify Kudelski Security in writing within ten business days after the completion of the services. Kudelski Security will have 30 calendar days or mutually agreed upon timing to remedy any non-conforming services. Time expended in re-performance does not extend any warranty period. EXCEPT AS SET FORTH IN THIS SOW, KUDELSKI SECURITY MAKES NO OTHER, AND EXPRESSLY DISCLAIMS ALL OTHER, REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, WHETHER STATUTORY, EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY STATUTORY, EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, DURABILITY, TITLE, ACCURACY OR COMPLETENESS OR NON-INFRINGEMENT) RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF THE SERVICES, INCLUDING THE PERFORMANCE OF ANY HARDWARE OR SOFTWARE USED IN PERFORMING SERVICES AND ANY RESULTS TO BE OBTAINED FROM THE SERVICES. THIS DISCLAIMER AND EXCLUSION WILL APPLY EVEN IF THE EXPRESS WARRANTY AND LIMITED REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE. Client acknowledges that no employee of Kudelski Security or its affiliates is authorized to make any representation or warranty on behalf of Kudelski Security or any of its affiliates that is not expressly in this SOW. Kudelski Security has no obligation if the claim is the result of an unauthorized modification by Client or its agents, material change in Client's environment, abuse, misuse or damage outside the control of Kudelski Security.

6. Insurance. During the term of this SOW, Kudelski Security will maintain (a) the appropriate insurance coverage to cover liabilities which may arise from the SOW. Kudelski Security will, on Client's request, provide Client with relevant insurance coverage evidence.

7. Infringement.

7.1 Kudelski Security will indemnify, defend and hold harmless Client, its officers, directors, employees, agents, and affiliates from and against any third party claims ("Claim") that any accepted deliverable provided to Client under this SOW infringes a U.S. patent, copyright, trademark or trade secret provided that Client (a) promptly notifies Kudelski Security in writing of the Claim, (b) makes no admission of liability and does not take any position adverse to Kudelski Security, (c) gives Kudelski Security sole authority to control the defense and settlement of the Claim, and (d) provides Kudelski Security with full disclosure and reasonable assistance as required to defend the Claim.

7.2 In the event the deliverable or any portion of the deliverable may in Kudelski Security's reasonable opinion found to be infringing, Kudelski Security at its option and own expense may do the following: (a) secure for Client the right to continue the use of the infringing item, (b) replace the infringing item with a substantial equivalent non-infringing item, or (c) modify the item to be non-infringing. In the event Kudelski Security is unable to perform the options previously listed (a) through (c), Client will then return the deliverable to Kudelski Security and Kudelski Security will refund Client the amount paid for such item. This infringement section 7 is Kudelski Security's entire liability and Client's sole and exclusive remedy with respect to any infringement or claim of infringement.

7.3 Kudelski Security will have no indemnification obligations where: (i) the deliverable was created in accordance with Client's sole design or specifications, (ii) Client alters the deliverable without Kudelski Security's prior written agreement, (iii) Client combines the deliverable with materials not supplied or approved by Kudelski Security and such infringement would not have occurred absent such combination, or (iv) Client continues to use the deliverable after receiving written notice from Kudelski Security to stop using the deliverable.

8. Limitation of Liability. Neither party will be liable to the other party for any indirect, special, incidental or consequential damages (for example, loss of profits or revenue, loss of or use of data, rework, repair, injury to reputation or loss of customers) under this SOW. the foregoing limitation applies regardless of the form of action or theory of relief, even if advised of the possibility of such damages. Except for claims of non-payment, the amount of direct damages recoverable from a Party for all claims is limited to the total amount paid or to be paid by the Client under this SOW. Except for claims of non-payment, any claim against Kudelski Security and its affiliates, of whatever nature, must be brought within one year of completion of the services.

9. Backup and Security. Client has the sole responsibility for the adequate protection and backup of systems, software and data that may be impacted by the services. Client will, among other measures, establish a backup procedure enabling Client to restore systems, software and data that existed before the start of services by Kudelski Security or its authorized subcontractors.

10. Third Party Software. For any services where Client is accessing or using third party software applications , Client agrees to any terms of "use" ,"click-thru" or license either displayed or incorporated as a result of using the third party software. Any terms of use are between the licensor or publisher of the software and Client.

11. Confidential Information.

11.1 "Confidential Information" means information disclosed by one Party to the other Party either directly or indirectly, in writing, orally or by drawings or inspection of samples, equipment or facilities; including (a) information identified by the disclosing Party, in writing or orally, as confidential at the time of disclosure; (b) information relating to the disclosing Party's technology, products, solutions and services used, provided and/or owned by the disclosing Party, including without limitation, technical data, trade secrets, know-how, research, product plans, ideas or concepts, products, services, software, inventions, patent applications, techniques, processes, developments, algorithms, formulas, technology, designs, schematics, drawings, engineering and hardware configuration information, operations, business and financial results or financial plans or strategies, including but not limited to Client, customer lists, markets, financial statements and projections, product pricing, marketing information, financial or other strategic business, plans or information; and (c) the content and terms of the SOW. Information is not deemed Confidential Information if it (i) is known to the receiving Party before receipt from the disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party, (ii) becomes known (independently of disclosure by the disclosing Party) to the receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party, (iii) becomes publicly known or otherwise ceases to be confidential, except through a breach of the SOW by the receiving Party, or (iv) is independently developed by the receiving Party.

11.2 Neither Party will use or disclose Confidential Information from the other Party without the prior written consent of the other Party except where (i) if in the documented opinion of counsel shared with Client, the disclosure is required by applicable law or regulation (including securities laws regarding public disclosure of business information) or by an order of a court or other governmental body having jurisdiction after taking steps to maintain its confidentiality where practicable including giving Kudelski Security advanced written notice and opportunity to intervene and seek a protective order for the disclosure; or (ii) reasonably necessary to be made to that Party's, or its affiliates', employees, officers, directors, consultants, attorneys, accountants and other advisors, or (iii) necessary for a Party to perform its obligations under this SOW.

11.3 Kudelski Security and Client will restrict disclosure of Confidential Information to only those personnel who have a need to know and will bind the personnel to obligations of confidentiality to the same extent that each Party is bound under this

SOW, and each Party warrants that it has the right to disclose the information it discloses. Upon written request by either Party, the other Party will promptly return all Confidential Information, including copies, to the disclosing Party of the Confidential Information.

12. Force Majeure. Kudelski Security is not liable for failure to fulfill its obligations under this SOW due to causes beyond its reasonable control (for example, acts of nature, acts or omissions by the Client, operational disruptions, man-made or natural disasters, epidemic medical crises, carrier delays, strikes, internet or telecommunication interruptions, criminal acts, delays in delivery or transportation, or inability to obtain labor, or materials).

13. Non-solicitation and Non-Hire. Client agrees that, without Kudelski Security's prior written consent, during the term of this SOW and for a period of 12 months following its expiration or termination, Client will not, nor will it permit any third party engaged by or otherwise affiliated with Client, to directly or indirectly solicit, divert or otherwise take away any employee of Kudelski Security, who has been directly involved in the performance of the services or induce or attempt to induce such employee to terminate his/her employment with, or otherwise cease his or her relationship with Kudelski Security. This obligation does not apply where an employee of Kudelski Security has unilaterally responded to a general recruitment advertisement or hiring campaign that was not specifically targeting such Kudelski Security employee.

14. Assignment, Subcontracting and Successors. Client may not assign this Agreement, or any of its rights or obligations without the prior written consent of Kudelski Security. Kudelski Security may assign or subcontract all or any portion of its rights or obligations related to this SOW, or assign the right to receive payments without Client's consent and without notice. Subject to the restrictions in assignment contained in this provision, this SOW binds and benefits the parties and their respective successors and assigns. Client will notify Kudelski Security immediately upon any change in ownership of more than fifty percent of Client's voting rights or any controlling interest in Client. If Client fails to do so or Kudelski Security objects to the change, Kudelski Security may terminate this SOW, require Client to provide adequate assurances, and/or put in place additional controls for Kudelski Security Confidential Information.

15. Arbitration and Governing Law. Any dispute, controversy or claim arising out of or in relation to this SOW, including the validity, invalidity, breach or termination, will be resolved by arbitration in Lausanne, Switzerland arbitration in accordance with the Swiss Rules of International Arbitration of the Swiss Chambers of Commerce. The number of arbitrators shall be one. The arbitral proceedings shall be conducted in English. The arbitral award shall be final and binding on the parties and shall include the questions of legal fees, costs of arbitration and all matters related thereto. This SOW is governed by the laws of Switzerland, without regard to its choice of law provisions. The Parties agree that the United Nations Convention on Contracts for the International Sale of Goods (CISG) does not apply to this SOW. Notwithstanding the foregoing, for any dispute, controversy or claim arising out of or relating to amounts due to Kudelski Security related to the services, Kudelski Security is not bound by this arbitration requirement and may at it sole option, seek to collect any amounts by legal means available including filing suit in any court with jurisdiction.

16. Miscellaneous. No provision of this SOW may be waived, amended or modified by either Party except by a written agreement signed by authorized representatives of both Client and Kudelski Security. The Parties agree that electronic signatures may be used and will be legally valid, effective, and enforceable. Any delay or failure by either Party to exercise any right or remedy will not constitute a waiver of that Party to enforce its rights. The relationship between Kudelski Security and Client is that of independent contractors and not that of employer-employee, partnership or joint venture. All rights and obligations of the Parties under this SOW automatically terminate with completion of services, except for payment obligations or other terms which by their nature are intended to survive termination including limitation of liability, warranty disclaimers, and this survival provision. If any part of this SOW is found by a court of competent jurisdiction to be invalid, illegal or unenforceable, all other parts will still remain in effect. Headings in this SOW are for reference purposes only and are not to be interpreted as being part of this SOW. Notices provided under this SOW must be in writing and be sent by registered or overnight carrier. Notice to Kudelski Security will be sent to: Nagravision S.A. – Kudelski Security, 22-24 rte de Genève, CH-1033 Cheseaux-sur-Lausanne, Switzerland, Attn: Legal Department..

EXHIBIT A: CONSULTANT PROFILES

Dr. Jean-Philippe Aumasson, Principal Research Engineer, Kudelski Security

JP has worked for the Kudelski Group since 2010 in the domains of cryptography and cybersecurity. He holds a PhD from EPFL, obtained in 2009.

In his work for Kudelski Security, Dr. Aumasson has designed and performed reviews of proprietary cryptographic components and implementations. He has also evaluated third-party encryption solutions in the course of consulting engagements, including secure communications solutions.

His published work and open-source contributions include:

- The widely used cryptographic algorithms SipHash and BLAKE2.
- The Cryptography Coding Standards, a reference of secure coding rules for cryptographic applications (https://cryptocoding.net).
- Conference presentations at top-tier venues such as Black Hat, DEF CON, or RSA Conference, or Chaos Communications Congress.
- The discovery of the first security vulnerabilities in the Signal mobile application, jointly with researcher Markus Vervier.
- Serious Cryptography (2017): book about crypto, published by No Starch Press
- SGX review (2016): research presented at Black Hat about Intel SGX
- The Hash Function BLAKE (2015): book about the hash function BLAKE, published by Springer
- NORX (2014): authenticated cipher candidate in the CAESAR competition
- Password Hashing Competition (2013-2015): open competition that selected Argon2 as a winner
- BLAKE2 (2013): hash function faster than SHA-2 and SHA-3, available in OpenSSL, Sodium, Crypto++, etc.
- Cryptography Coding Standard (2013-): coding rules to prevent common weaknesses in cryptography software
- SipHash (2012): keyed hash function, used in Linux, FreeBSD, OpenBSD, Python, among others

Dr. Tommaso Gagliardoni, Cryptography Expert, Kudelski Security

Tommaso is a member of the research team at Kudelski Security. He studied mathematics at the University of Perugia, Italy, and obtained a PhD in cryptography from the Technical University of Darmstadt, Germany, under supervision of Prof. Marc Fischlin. He worked previously at IBM Research Zurich in the group of renown cryptographer Dr. Jan Camenisch. His area of expertise is cryptography, quantum security, and privacy. He has spoken at top tier IACR scientific conferences such as CRYPTO, EUROCRYPT, ASIACRYPT, and PKC.

His published works and activities include:

- Analysis of the limits of cryptographic security against quantum computers (in respect to techniques such as group homomorphic encryption, length-preserving block ciphers, signatures of quantum states, etc.)
- Design and analysis of numerous cryptographic algorithms able to run natively on a quantum computer.
- A practical solution to the longstanding problem of securely authenticating quantum data.
- Cryptographic audit of the smart-card authentication protocol ESORICS.
- Cryptanalysis and hack of the ISO standard smart-card authentication protocol PLAID used by the Australian government and healthcare sector.
- Advances in fundamental cryptographic techniques such as universal composability and Fiat-Shamir.
- Tutorials and invited talks at venues like the Italian E-privacy conference and the International Journalism Festival on the safe use of cybersecurity tools for investigative journalist in low-democracy geopolitical situations.
- Continuous involvement in cryptographic academic activities (conference program chair, referee, organization of schools and seminars) and H2020 projects.

Yolan Romailler, Research Engineer, Kudelski Security

Yolan is a Security Researcher at Kudelski Security, specialized in cryptography, secure coding, blockchains and vulnerability research. Yolan first graduated in mathematics at EPFL and later in computer sciences and information security. He has spoken at Black Hat, BSidesLV and DEF CON, and presented at FDTC 2017 ("Fault Diagnosis and Tolerance in Cryptography") the first known practical fault attack against the EdDSA signature scheme.

His published work and open-source contributions include:

- The first practical fault attack against the Ed25519 and EdDSA signature schemes.
- The largest public key collection and study to date, presented at DEF CON 2018.
- Crypto Differential Fuzzer, which he presented at Black Hat 2017 and whose code is open-source.
- A Go implementation of the timing leaks’ detection method called Dudect.
- Open source code to conduct Manger's attack with generic oracles.
- A wrapper in Go to operate garbled circuits with TinyGarble.

EXHIBIT B: KUDELSKI SECURITY OVERVIEW

A Global Provider of Cybersecurity Solutions

Kudelski Security is the premier advisor and cybersecurity innovator for today's most security-conscious organizations. Our long-term approach to client partnerships enables us to continuously evaluate their security posture to recommend solutions that reduce business risk, maintain compliance and increase overall security effectiveness. With clients that include Fortune 500 enterprises and government organizations in Europe and across the United States, we address the most complex environments through an unparalleled set of solution capabilities including consulting, technology, managed security services and custom innovation.

Kudelski Security leverages almost 30 years of the Kudelski Group's expertise and investments in digital security-related innovation, cryptography, monitoring and research to develop a unique solutions platform in demand around the world.

Kudelski Security has direct access to the Group's pool of more than 2 000 talented R&D engineers. Its teams of experts use a combination of technology, innovation, and services capabilities to empower organizations to build, deploy and manage effective cybersecurity programs.

Innovation is in our DNA. We have been innovating for over 20 years to create solutions to complex media security challenges. The Kudelski Group holds over 5000 patents and is home to a large team of multi-disciplinary experts covering everything from cryptography and cloud security to big data science and advanced networking. Partnerships with top academic institutions around the world enrich our research and take it to a wider audience.

Cryptography is a critical component of modern systems, ensuring secure communications, data confidentiality, and program integrity. Since its founding in 1951, the Kudelski Group has been a market leader in cryptography engineering and research, providing services to secure and monetize digital content. Extending this expertise to our broader base of cybersecurity clients, we offer services that span a wide range of areas, including algorithm design (proprietary ciphers for smart cards, popular open-source designs such as BLAKE2), implementation (efficient software and hardware code, side-channel defenses), and review (review of third-party products, source code audits).

Kudelski Security's global reach and cyber solutions focus are reinforced by key international partnerships. These include alliances with the world's leading security technology companies that are aligned with internal industry experts focused on offering clients the tools, knowledge and methodologies they need to meet any cybersecurity challenge they face.

Kudelski Security is ISO 27001:2013 certified, ensuring the quality of our Information Security Management System to protect client data while delivering cyber security solutions.

Furthermore, Kudelski Security is a member of the Forum of Incident Response and Security Teams (FIRST), a premier organization and recognized global leader in incident response and Computer Emergency Response Team (CERT) competencies.

For more information visit: www.kudelskisecurity.com.

EXHIBIT C: KUDELSKI GROUP OVERVIEW

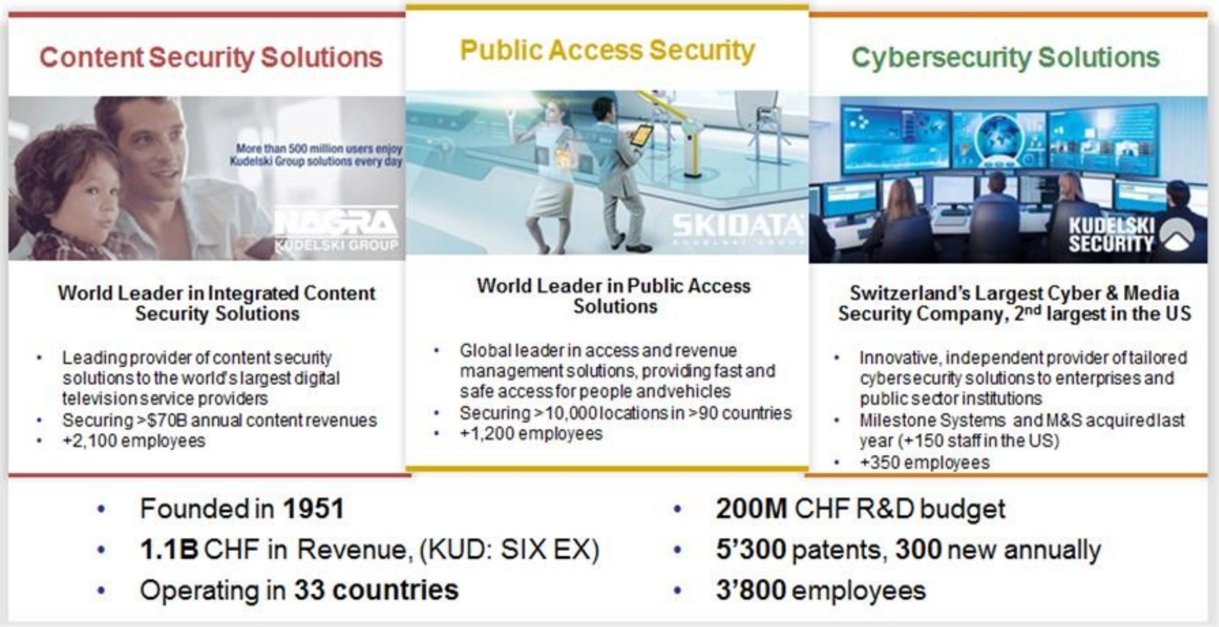
A Global Technology Leader

The Kudelski Group, based in Cheseaux, Switzerland and Phoenix, Arizona, is the world leader in the development and delivery of state-of-the-art technologies to secure the revenues of content owners and service providers for digital television and interactive applications across all network types. The Group's solutions enable consumers to access content seamlessly over any device through an exciting viewing experience.

Leveraging its long-standing expertise in securing digital content and fighting piracy, the Group is also a global provider of cybersecurity solutions and services focused on protecting companies' and organizations' data and systems.

The Kudelski Group capitalizes on its 5 300 patent-rich intellectual property portfolio through licensing arrangements that involve state-of-the-art technology portfolios, demonstrating the relevance of the Group's innovation and the key role it is playing in the industries in which it operates.

The Kudelski Group is also a leader in public access solutions. The world's largest parking facilities, stadiums and mountain resorts use SKIDATA's integrated people and vehicle management solutions. The Kudelski Group employs 3,800 people in 33 countries around the world. For more information, please visit www. nagra.com.


More than 500 million users enjoy Kudelski Group solutions every day
NAGRA
KUDELSKI GROUP
SKIDATA
KUDELSKI SECURITY

Content Security Solutions

World Leader in Integrated Content Security Solutions

- Leading provider of content security solutions to the world's largest digital television service providers
- Securing >$70B annual content revenues
- +2,100 employees

Public Access Security

World Leader in Public Access Solutions

- Global leader in access and revenue management solutions, providing fast and safe access for people andvehicles
- Securing >10,000 locations in >90 countries
- +1,200 employees

Cybersecurity Solutions

Switzerland's Largest Cyber & Media Security Company, 2nd largest in the US

- Innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions
- Milestone Systems and M&S acquired last year (+150 staff in the US)
- +350 employees

- Founded in **1951**
- **1.1B** CHF in Revenue, (KUD: SIX EX)
- Operating in **33 countries**
- **200M** CHF R&D budget
- **5'300** patents, **300** new annually
- **3'800** employees