Monero Distribution Company (Pty) Ltd

Software Security Assessment Services

Source code audit: Bulletproofs protocol

February 06, 2018
Version: 2.0

Presented by:

Jennifer de Broglie
Key Account Manager, EMEA
Kudelski Security

Route de Genève, 22-24
CH-1033 Cheseaux
jennifer.debroglie@kudelskisecurity.com

To:

Sarang Noether
Monero Distribution Company (Pty) Ltd
Boston Light Drive, Plettenberg Bay,
Western Cape, South Africa, 6600

+27 72 888 7774 / +1-701-630-9396
sarang.noether@protonmail.com

KUDELSKI SECURITY

TABLE OF CONTENTS

FORWARD

Thank you very much for this opportunity to serve Monero Distribution Company. We are pleased to make the following proposal for security assessment services and look forward to proving to you our excellence and professionalism in this field.

In this offer, we have made every effort possible to provide you with accurate, relevant, and comprehensive information in order to facilitate and maximize your evaluation process. That said, should you have any questions or require additional clarification on any of the services described herein, please do not hesitate to reach out to us.

Kudelski Security is committed to delivering the solutions that will help you chart a successful course toward cyber maturity. On behalf of the entire Kudelski Security team, we would be much honored to begin working with you to help strengthen the security of the Monero Bulletproof's protocol.

We have availability to begin the mission per your requirements (March 2018) and hope that the following information will help you make a positive decision on our offer.

Best Regards,

Jennifer de Broglie (MBA/CISM)
Account Executive – EMEA
Kudelski Security
jennifer.debroglie@kudelskisecurity.com
+41 79 249 1250

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.

KUDELSKI GROUP OVERVIEW

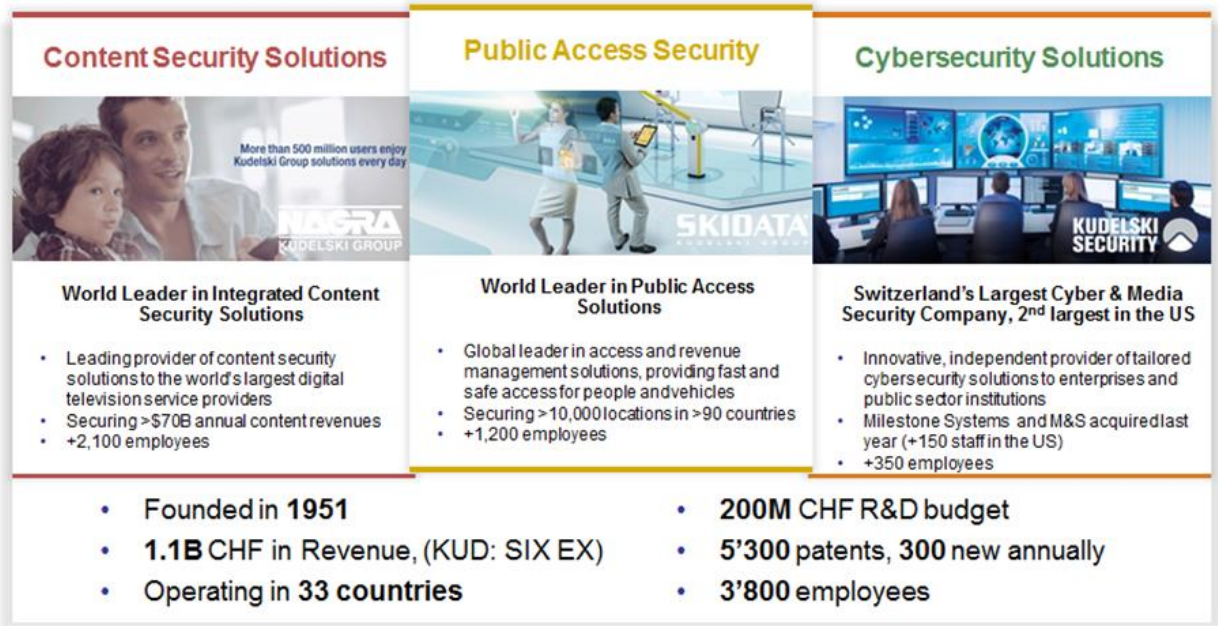
A global technology leader

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



KUDELSKI SECURITY

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.

The Monero Cryptocurrency uses Ring Confidential Transactions (ringCT) to hide the amounts being transacted on its blockchain. One of the consequences of hiding amounts is that you still need a means of verifying that the amounts are legitimate, don't overflow, etc., without revealing them. In CT, "range proofs" are used to assert the validity of output amounts. These proofs are quite large, causing a typical 1-input/2-output Monero transaction to use around 12.5kB. (Pre-ringCT this transaction would be only around 500 bytes.)

Last November 2017 saw the release of new work out of Stanford called "Bulletproofs" which makes the size of a range proof logarithmic in the number of values, instead of the linear size they currently consume. Use of Bulletproofs is expected to reduce typical Monero transaction sizes by ~80%, representing a significant improvement. The Monero Research Lab developed a prototype in Java, and The Monero Project has subsequently implemented Bulletproofs in C++ and this code has been running on the Monero testnet since the beginning of last December.

While the researchers in the Monero Research Lab are confident in the soundness of the math in the Bulletproofs paper, the Monero Project is being cautious about deploying the feature to production on mainnet. The Monero Project recognizes the value of independent 3rd-party reviews. Therefore, the Monero Project is now soliciting help in conducting formal, in-depth reviews of the C++ implementation.

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

Following discussions with Sarange Noether, Monero Distribution Company, and JP Aumasson, Principal Research Engineer, Kudelski Security, an offer for a comprehensive security audit of the Bulletproofs 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 Senior Program Manager, Kudelski Security has identified the following engagement objectives:

- Help Monero users and developers to better understand the current risks and security postures of their software components.
- Provide a professional opinion on the maturity, adequacy and efficiency of the security measures that are in place within the Bulletproof protocol.
- 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

- Audit source code or technical specifications for security defects and improvement opportunities;
- Review the underlying cryptographic components as well as their implementations' strength.
- Provide remediation recommendations and support and perform re-testing.

Key Points

- The mission will be conducted by Dr. Jean-Philippe Aumasson, a renowned cryptography expert, supported by Yolan Romailler, Cryptography and Research Engineer.
- For this mission, estimated at ≈ 10-12 days, a daily rate of USD 2'500 is applied to both cryptographers for a total mission cost not to exceed USD 30'000. This special rate (discounted 15%) represents our strong desire to work with you on this prestigious project.
- Most of the work can be delivered remotely. On-premise work is possible as needed/requested.
- We have availability to complete this mission in March 2018.

Engagement Deliverables

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

Engagement Location

The engagement will be executed remotely with on-site execution as required at the following location: TBD.

ENGAGEMENT SCOPE AND ACTIVITIES

Engagement Preparation

Prior to the start of the engagement, Kudelski Security will host and lead a kickoff call with Monero ' 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:

1. Finalize the mission scope and timelines for the engagement's commencement and duration.
2. Validate that goals and scope are accurately captured in the Statement of Work.
3. Ensure activities are understood and coordinated prior to commencement.
4. Identify any obstacles or challenges to completion that may be unique to Monero .
5. Identify key stakeholders from both Kudelski Security and Monero who need to be included in the engagement updates and escalations.
6. Agree on secure communication path.
7. Sign the Statement of Work.

Engagement Description

The intent of the Software Security Assessment is to understand the security level of the Bulletproofs technology.

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 components?
- Can the product or and its protocols or their implementations be abused by attackers?

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 on-site presentation, including relevant data and recommendations to guide the prioritized remediation.

Detailed Scope

Based on your discussions with Jean-Philippe Aumasson, we estimate that we can complete the audits within twelve (12) days. Further ten-day work packages can be ordered on a pay-as-you-go basis. This contract covering the first 12 days of work can be extended, as needed.

Security Assessment work packages are typically performed according to the following workload table. The time estimated below is based on your first project, described in the executive summary.

Detailed Scope	Workload
Preparation, Exploration, Documentation Tasks: • Grasp the codebase • Review the bulletproof documentation • Setup testing • Finalize Statement of Work (SoW) and hold the kick-off meeting. Deliverables: • Statement of Work (SoW).	2 md
Code review and reporting Tasks: • Review bulletproof code and it's direct dependencies • Test and review the tests done and try some more tests, to ensure correctness Deliverables: • Technical report describing issues identified and mitigation recommendations • Informal description of any critical issue prior to the report delivery	6-7 md
Final Client Audit Report and Presentation Tasks: • Summarize discovery, structured attack scenarios and results. • Professional opinion on the security posture of the application. • Recommendations to fix identified vulnerabilities. • Present and explain the suggested recommendations. • Provide remediation support. Deliverables: • Technical report detailed the findings, executive summary and a remediation plan composed by actionable recommendations.	2-3 md
TOTAL	10-12 md

ENGAGEMENT DELIVERABLES

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

Kudelski Security will provide Monero with the following deliverables in electronic format, as follows:

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

Kudelski Security will deliver the Executive Summary presentation to Monero stakeholders per agreed timeline either on-site in Prague or remotely, per client instruction.

Deliverable Acceptance

All deliverables defined in this offer are subject to inspection and acceptance by the designated Monero Designated Contact.

There will be one (1) round of draft review, during which Monero 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 acceptance or rejection. In the event that the deliverable does not conform to the agreed-upon acceptance requirements, Monero shall notify Kudelski Security in writing, setting forth Monero rejection and the basis of the nonconformity. Kudelski Security shall correct such nonconformity within a mutually agreeable timeframe.

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

Scheduling

Kudelski Security has availability for Monero to begin this engagement within 30 days of acceptance of the offer.

Rescheduling or Cancellation

Two (2) weeks' written notice in advance of cancelling or rescheduling the consultant resource is requested. Notices can be sent to Jennifer.debroglie@KudelskiSecurity.com.

ENGAGEMENT RESPONSIBILITIES

Kudelski Security Responsibilities

Kudelski will:

- Directly manage Kudelski Consultants and Project Managers, excluding any Monero contracted consultants or third parties, unless agreed to in writing.
- Follow all reasonably written security rules and procedures provided by Monero .

KEY PERSONNEL

NAME	FUNCTION	PHONE	EMAIL
Monero CONTACT			
Sarang Noether		+27 72 888 7774 / +1-701-630-9396	sarang.noether@protonmail.com
KUDELSKI SECURITY CONTACTS			
Jennifer de Broglie	Key Account Executive, EMEA	+41 79 249 12 50	Jennifer.debroglie@kudelskisecurity.com
JP Aumasson	Principal Research Engineer	+41 79 726 05 08	Jp.aumasson@kudelskisecurity.com
Yolan Romailler	Cyber Security Research Engineer	+41 79 647 56 47	Yolan.romailler@kudelskisecurity.com

ENGAGEMENT PRICING

Financial Terms

We estimate that the required workload to successfully perform this mandate is 10 to 12 days. Kudelski Security applies the following man day rate which takes into account the estimated volume of up to 12 man days.

The mission cost includes all the relevant human resources of the following profiles:

Profile	Man day rate
Principal Research Engineer, cryptography & cybersecurity	USD 2'500 (two thousand five hundred US dollars)
Research Engineer, cryptography vulnerability	USD 2'500 (two thousand five hundred US dollars)

Please note that if the workload increases for this or any other mandate for Monero, volume discounts will apply.

invoices will be sent end-of-month for the work performed during the month, with a maximum of 15 man days per month per consultant assigned to the mission.

Should Monero require additional resources or complementary skill sets, Kudelski Security will submit separate commercial offers for approval and apply the same volume discounts.

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.

1. The consultants will be under the responsibility and direct management of Kudelski Security Project Managers.
2. Travel and accommodation will be invoiced at cost and separately with justification elements.
3. Kudelski Security will respect Monero travel and accommodation policies for the expenses incurred over the course of the engagement.
4. Invoices will be produced on a monthly basis.
5. Terms are net 30 days.
6. Any additional services proposed during the engagement will be subject to a separated commercial offer and to Monero approval before proceeding.
7. 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.

8. A bilateral non-disclosure agreement will be agreed and signed by both parties prior to initiating the project.

Acceptance

We confirm that this proposal has been validated and is signed by duly authorized representatives of Nagravision SA on behalf of the Kudelski Security division.

Please submit by post two original signed copies of this proposal to Kudelski Security and scan and send a copy to Jennifer de Broglie to reserve the resources and to accelerate the launch of the project.

I confirm my agreement with the terms and conditions described in this service proposal.

Nagravision SA on behalf of Kudelski Security	**Monero**
_____	_____
Authorized Signature	Authorized Signature
	_____
	Name (Print)
	_____
	Title
_____	_____
Date	Date

Appendix: 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

Work samples

IOHK

https://twitter.com/IOHK_Charles/status/955476966798327809

https://research.kudelskisecurity.com/2018/01/26/audit-report-of-iohks-etc-wallet/

Waves

https://research.kudelskisecurity.com/2017/10/10/audit-report-of-the-waves-platform/

Wire

https://www.x41-dsec.de/security/report/2017/02/09/projects-x41-wire/

My book

https://www.amazon.com/Serious-Cryptography-Practical-Introduction-Encryption/dp/1593278268/

Yolan Romailler, Research Engineer, Kudelski Security

Yolan Romailler is a Research Engineer at Kudelski Security since 2017, specialized in cryptography vulnerability research. Yolan has a background in mathematics, which he studied at EPFL, and he earned a master in computer sciences and information security from the HES-SO, Switzerland. The topic of his Master's thesis was automated testing of cryptographic software. He tweets as @anomalroil.