onXRP Audit Report

FINAL –04.24.2023

TABLE OF CONTENTS

Executive Summary

Brief overview of the audit

This report presents the findings from a comprehensive audit of onXRP's key management and cryptographic security practices. The audit was conducted to assess the security of the key management infrastructure, and identify potential vulnerabilities.

Purpose and scope of the audit

The purpose was to ensure that onXRP's cryptographic key management system adheres to industry best practices and provides adequate security for its customers. The audit scope included a system architecture review, basic source code review, public key verification, and recommended improvements.

Background of onXRP

onXRP is a blockchain-based signing solution that leverages AWS Key Management Service (KMS) to generate, store, and manage encryption keys securely. Their system is designed to provide a high level of security for transactions and data through the proper management and protection of cryptographic keys.

Importance of key management

Effective key management is crucial to the security of any cryptographic system, as it ensures the confidentiality, integrity, and availability of cryptographic keys. Proper key management practices help prevent unauthorized access to sensitive data, protect the integrity of transactions, and maintain the system's overall security.

Reviewer Background

The audit was conducted by BuildTomorrow and Garantir. BuildTomorrow's and Garantir's teams comprise experienced cybersecurity professionals with strong cryptography and key management backgrounds. We have conducted numerous audits for various clients, ensuring their systems comply with industry standards and best practices. The review was primarily performed by Kieran Miller, Security Chief Architect, who has worked in cryptographic key management for over 15 years, with experience in both Department of Defense (DoD) and commercial world key management applications.

Intended Audience

This report is intended for the onXRP management team, security professionals, and any stakeholders involved in the decision-making process for security improvements and key management practices. It is assumed that the readers of this document and the users of its content have a strong understanding of:

- Security concepts including, but not limited to, authentication, authorization, digital signatures, logging, separation of duties, and preventative/detective controls

- Computer networking

- Cryptographic Tokens (e.g., hardware security modules)

Audit Methodology

Standards and guidelines followed

The audit was conducted following industry best practices and widely recognized standards, such as the National Institute of Standards and Technology (NIST) Special Publication 800-57 for key management and the International Organization for Standardization (ISO) 27001 for information security management systems. These guidelines provided a comprehensive framework for evaluating onXRP's key management infrastructure and identifying areas for improvement.

Audit approach

The audit approach consisted of a combination of interviews, documentation review, and testing to thoroughly understand onXRP's key management practices and identify potential vulnerabilities. The process involved:

- Conducting interviews with key personnel to understand their roles and responsibilities in the key management process. Interviews were conducted with the key technical team members who developed and operated the infrastructure.

- Reviewing documentation related to key management policies, procedures, and architecture.

- Assessing the security of onXRP's system architecture, including cryptographic key management.

- Reviewing source code for implementation flaws related to private key usage through manual code review and static code analysis.

- Verifying the strength of public keys and the security of private keys by matching them with the public keys verified from the customer's KMS.

Limitations and assumptions

While the audit aimed to provide a comprehensive assessment of onXRP's key management practices, there were some limitations and assumptions:

- The audit focused on the key management infrastructure and did not include an exhaustive review of onXRP's security posture.

- This review was done at a single point in time. Changes can be made to the environment after the fact that significantly increases or decreases the security of the key management. Additionally, external factors such as employee background checks, and endpoint protection can evolve.

- It was assumed that the information provided by onXRP personnel during interviews and documentation review was accurate and complete.

- The audit was conducted within a limited timeframe, which may have restricted the extent of the analysis.

Key Management Lifecycle

Key generation

As of the time of authoring this document, onXRP uses two keys. Both keys are secp256k1 keys, but the first key is stored in AWS Secrets Manager while the second key is stored in AWS Key Management Service (KMS). The Secrets Manager key is exported in plaintext format to the application server (over TLS) when it is used, while the KMS key is generated, stored, and used in a FIPS 140-2 certified HSM in a non-exportable manner.

Key distribution

As it relates to the signing keys, only the Secrets Manager key is distributed anywhere, the KMS key is not. We cannot fully guarantee that the Secrets Manager key has only been sent to authorized entities or has always been transmitted securely. Given the nature of exported keys - once they are exported, it is difficult to guarantee their safety. However, we found nothing in onXRP's source code or environment to suggest the key has been compromised or mishandled.

As it relates to authentication keys (i.e., the keys used to authenticate to services like KMS and Secrets Manager), the ones we audited were properly controlled via IAM roles but there could be other ones out there that are not properly controlled or protected. Similar to above, we found nothing to suggest that any authentication keys have been compromised or mishandled.

Key storage and protection

It is possible for an attacker to compromise the Secrets Manager private key bytes but it is not practical for an attacker to do the same to the KMS private key bytes. Therefore, with respect to key protection, any wallet solely protected by the Secrets Manager key would be less secure than any wallet solely protected by the AWS KMS key. It is important to note that a wallet that is protected by both the AWS KMS key and the Secrets Manager key (i.e., a wallet where both keys must be used to sign a transaction on its behalf) is at least as secure as the more secure key (i.e., the AWS KMS key), and likely even more secure.

Key usage

The audit reviewed the usage of cryptographic keys within onXRP's system to ensure that keys are used only for their intended purposes and within appropriate limits. It was determined that, although the application with access to the KMS key does not perform full validation of the data it signs, this risk is mitigated by strong authentication performed by AWS API Gateway and the calling application.

Key rotation and replacement

The audit considered onXRP's approach to key rotation and replacement. There are no plans for key rotation, but this is mitigated by NIST's ongoing development of post-quantum cryptographic algorithms and the expected support from HSM and cloud vendors. onXRP should implement a plan for key rotation once these new algorithms become available and industry standards are established.

Key revocation and destruction

The audit assessed onXRP's processes for key revocation and destruction to ensure that keys are properly retired and destroyed when no longer needed. While specific processes for key revocation and destruction were not observed during the audit, it is recommended that onXRP define and document these processes as part of their key management lifecycle. This will help to minimize the risk of unauthorized access to or misuse of outdated or compromised keys.

Conclusion

With the migration of all wallets to a threshold of 2 and their linkage to onXRP's AWS KMS key, onXRP's system now demonstrates a considerable improvement in the security of end-user wallets and transactions. This achievement is a testament to onXRP's commitment to maintaining a robust key management infrastructure and protecting its customers' assets.

The overall assessment of onXRP's key management practices is positive. onXRP has implemented various security measures and demonstrated a clear understanding of the importance of secure key management.

We would like to acknowledge and appreciate the cooperation and support from the onXRP team throughout the audit process. Their dedication to addressing security concerns and willingness to improve their system has been invaluable in achieving a successful audit

outcome. We hope the insights provided in this report will serve as a valuable resource for onXRP as they strive for excellence in security and key management.