A Survey of Tokenization Methods

Daniel Ayala Zamorano Laura Natalia Borbolla Palacios
Ricardo Quezada Figueroa

June, 2018

Abstract

When the online commerece begin to arise, the credit card frauds become a very frequent problem. For this reason, the Payment Card Industry (PCI) Secuirity Standard Council (SSC), did a standard for rule the function of any entity related with the processing of payments through the internet. This standard has a lot of requirements, and for a small store, it's hard and expensive to be PCI compliance. In the last years, a process named tokenization has become a very popular solution for online stores to reduce their PCI scope. Regretabbly, there is a lot of misinformation around this subject and the PCI guides to tokenization don't help to clarify. In this paper we explain what tokenization is and its relation to cryptography. Over this line, we point out what is the problem with PCI DSS clasification and provide a more logic one. We analyze and compare the more common tokenization methods and conclude with a discussion on the advantages and disadvantages of each one.

1 Introduction

2 Preliminaries

3 Reversible methods

3.1 FFX

References: [1]–[3]. Format-preserving Feistel-based Encryption (FFX).

3.2 BPS

References: [4]. Brier-Peyrin-Stern (BPS).

4 Irreversible methods

4.1 TKR

References: [5].

4.2 RHA

References: [6]. Reversible Hybrid Algorithm (RHA).

4.3 UTO

References: [7]. Updatable Tokenization (UTO).

4.4 DRBG

References: [8]. Deterministic Random Bit Generator (DRBG).

5 Experimental results

6 Conclusion

References

[1] Mihir Bellare, Phillip Rogaway, and Terence Spies. "The FFX Mode of Operation for Format-Preserving Encryption". Version 1.0. In: (2009) (cit. on p. 1).

[2] Mihir Bellare, Phillip Rogaway, and Terence Spies. "The FFX Mode of Operation for Format-Preserving Encryption". Version 1.1. In: (2010) (cit. on p. 1).

[3] Phillip Rogaway. *A Synopsis of Format-Preserving Encryption*. 2010. URL: `http://web.cs.ucdavis.edu/~rogaway/papers/synopsis.pdf` (cit. on p. 1).

[4] Eric Brier, Thomas Peyrin, and Jacques Stern. "BPS: a Format-Preserving Encryption Proposal". In: (2010) (cit. on p. 1).

[5] Sandra Diaz-Santiago, Lil María Rodríguez-Henríquez, and Debrup Chakraborty. "A cryptographic study of tokenization systems". In: *Int. J. Inf. Sec.* 15.4 (2016), pp. 413–432. DOI: `10.1007/s10207-015-0313-x`. URL: `https://doi.org/10.1007/s10207-015-0313-x` (cit. on p. 2).

[6] Riccardo Aragona, Riccardo Longo, and Massimiliano Sala. "Several proofs of security for a tokenization algorithm". In: *Appl. Algebra Eng. Commun. Comput.* 28.5 (2017), pp. 425–436. DOI: 10.1007/s00200-017-0313-3. URL: https://doi.org/10.1007/s00200-017-0313-3 (cit. on p. 2).

[7] Christian Cachin, Jan Camenisch, Eduarda Freire-Stögbuchner, et al. "Updatable Tokenization: Formal Definitions and Provably Secure Constructions". In: *Financial Cryptography and Data Security - 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers*. 2017, pp. 59–75. DOI: 10.1007/978-3-319-70972-7_4. URL: https://doi.org/10.1007/978-3-319-70972-7_4 (cit. on p. 2).

[8] Elaine Barker and John Kelsey. *NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. 2015. URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1 (cit. on p. 2).