

How can an entity ensure that hashed and truncated versions cannot be correlated?

PCI SSC FAQ | Article 1308 | June 2025

PCI DSS Requirement 3.5.1 states that if hashed and truncated versions of the same PAN, or different truncation formats, are present in the environment, additional controls must be implemented to prevent correlation.

The simplest solution is not to store both hashed and truncated PANs. If both must be retained, the following controls can help:

- Use of strong, unique, secret salts for hashing
- Separate storage systems for hashed and truncated values, isolated with segmentation, and distinct access controls
- Preventing cross-references or database links between values
- Real-time monitoring to detect correlation attempts

These are examples only. Controls should be suitable for the environment and ensure that full PAN reconstruction is not possible.

As per the guidance listed in PCI DSS implementing keyed cryptographic hashes with associated key management processes and procedures in accordance with Requirement 3.5.1.1 is a valid additional control to prevent correlation.

Source: <https://www.pcisecuritystandards.org/faqs/1308/>