

point of sale, particularly while ensuring the inclusion of proper cryptograms and additional data.

Thus, there is a need for a technical solution where a computing device can be properly configured to accommodate for transaction account numbers of
5 varying lengths while still including cryptograms and other data necessary for the use in payment transaction and staying within data limits.

SUMMARY

The present disclosure provides a description of systems and methods for enhanced validation of cryptograms for varying account number lengths.

10 A method for enhanced validation of cryptograms for varying account number lengths includes: storing, in a memory of a computing device, one or more primary account numbers and a plurality of formatting templates, wherein each template is associated with at least an account number length; receiving, by an input device of the computing device, a selection indicating a specific primary account
15 number of the one or more primary account numbers; executing, by a querying module of the computing device, a query on the memory to identify a specific formatting template of the plurality of formatting templates where the associated account number length corresponds to a length of the specific primary account number, and wherein the formatting templates include information specifying the
20 length and location of information to be included in a data string; receiving, by a receiving device of the computing device, at least an unpredictable number from a point of sale device; generating, by a generation module of the computing device, a cryptogram based on at least the unpredictable number and one or more algorithms; generating, by the generation module of the computing device, a data string, wherein
25 the data string includes at least the generated cryptogram, the specific primary account number, and the unpredictable number, and wherein the data string is formatted based on the identified specific formatting template; and electronically transmitting, by a transmitting device of the computing device, the generated data string to the point of sale device.

30 A system for enhanced validation of cryptograms for varying account number lengths includes: a memory of a computing device configured to store one or more primary account numbers and a plurality of formatting templates, wherein each template is associated with at least an account number length; an input device of the

computing device configured to receive a selection indicating a specific primary account number of the one or more primary account numbers; a querying module of

the computing device configured to execute a query on the memory to identify a specific formatting template of the plurality of formatting templates where the associated account number length corresponds to a length of the specific primary account number, the formatting templates including information specifying the length and location of information to be included in a data string; a receiving device of the computing device configured to receive at least an unpredictable number from a point of sale device; a generation module of the computing device configured to generate a cryptogram based on at least the unpredictable number and one or more algorithms, and a data string, wherein the data string includes at least the generated cryptogram, the specific primary account number, and the unpredictable number, and wherein the data string is formatted based on the identified specific formatting template; and a transmitting device of the computing device configured to electronically transmit the generated data string to the point of sale device.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

The scope of the present disclosure is best understood from the following detailed description of exemplary embodiments when read in conjunction with the accompanying drawings. Included in the drawings are the following figures:

FIG. 1 is a block diagram illustrating a high level system architecture for enhanced validation of cryptograms for varying account number lengths in accordance with exemplary embodiments.

FIG. 2 is a block diagram illustrating the computing device of FIG. 1 for the generation and providing of a data string for enhanced cryptogram validation for account numbers of varying lengths in accordance with exemplary embodiments.

FIG. 3 is a flow diagram illustrating a process for enhanced generation and validation of cryptograms for varying account number lengths using the system of FIG. 1 in accordance with exemplary embodiments.

FIG. 4 is a flow diagram illustrating a process for generation and conveyance of a data string for enhanced validation of a cryptogram for account numbers of varying lengths using the computing device of FIG. 1 in accordance with exemplary embodiments.

FIG. 5 is a diagram illustrating the varied formatting of a data string for the conveyance of cryptograms and other transaction data for account numbers of varying lengths in accordance with exemplary embodiments.

WHAT IS CLAIMED IS:

1. A method for enhanced validation of cryptograms for varying account number lengths, comprising:

storing, in a memory of a computing device, one or more primary account
5 numbers and a plurality of formatting templates, wherein each template is associated with at least an account number length;

receiving, by an input device of the computing device, a selection indicating a specific primary account number of the one or more primary account numbers;

executing, by a querying module of the computing device, a query on the
10 memory to identify a specific formatting template of the plurality of formatting templates where the associated account number length corresponds to a length of the specific primary account number, and wherein the formatting templates include information specifying the length and location of information to be included in a data string;

15 receiving, by a receiving device of the computing device, at least an unpredictable number from a point of sale device;

generating, by a generation module of the computing device, a cryptogram based on at least the unpredictable number and one or more algorithms;

generating, by the generation module of the computing device, a data string,
20 wherein the data string includes at least the generated cryptogram, the specific primary account number, and the unpredictable number, and wherein the data string is formatted based on the identified specific formatting template; and

electronically transmitting, by a transmitting device of the computing device, the generated data string to the point of sale device.

25 2. The method of claim 1, wherein

each formatting template of the plurality of formatting templates is further associated with a number of digits, and

the specific formatting template is identified based on a correspondence
between the associated number of digits and a number of digits of the received
30 unpredictable number.

3. The method of claim 1, wherein the generated data string is electronically transmitted in a data message that further includes a bitmap indicative of formatting of the generated data message.

4. The method of claim 3, further comprising:
5 generating, by the generation module of the computing device, the bitmap based on at least the identified specific formatting template.

5. The method of claim 3, wherein
each formatting template of the plurality of formatting templates further includes a bitmap, and
10 the bitmap included in the data message corresponds to the bitmap included in the identified specific formatting template.

6. The method of claim 1, wherein
the memory further includes, for each of the one or more primary account numbers, a transaction counter, and
15 the generated data string further includes the transaction counter associated with the specific primary account number.

7. The method of claim 6, wherein the cryptogram is further based on the transaction counter associated with the specific primary account number.

8. The method of claim 1, further comprising:
20 generating, by the generation module of the computing device, a second cryptogram based on at least the unpredictable number and at least one additional algorithm, wherein
the data string further includes the second cryptogram.

9. The method of claim 1, wherein the data string further includes at least
25 one extra digit, and where a number of extra digits is based on the length of the specific primary account number and a number of digits of the received unpredictable number.

10. The method of claim 9, wherein the at least one extra digit stores cardholder verification method data.

30 11. A system for enhanced validation of cryptograms for varying account number lengths, comprising:

a memory of a computing device configured to store one or more primary account numbers and a plurality of formatting templates, wherein each template is associated with at least an account number length;

an input device of the computing device configured to receive a selection indicating a specific primary account number of the one or more primary account numbers;

5 a querying module of the computing device configured to execute a query on the memory to identify a specific formatting template of the plurality of formatting templates where the associated account number length corresponds to a length of the specific primary account number, the formatting templates including information specifying the length and location of information to be included in a data string;

10 a receiving device of the computing device configured to receive at least an unpredictable number from a point of sale device;

a generation module of the computing device configured to generate a cryptogram based on at least the unpredictable number and one or more algorithms, and

15 a data string, wherein the data string includes at least the generated cryptogram, the specific primary account number, and the unpredictable number, and wherein the data string is formatted based on the identified specific formatting template; and

a transmitting device of the computing device configured to electronically transmit the generated data string to the point of sale device.

20 12. The system of claim 11, wherein each formatting template of the plurality of formatting templates is further associated with a number of digits, and

the specific formatting template is identified based on a correspondence between the associated number of digits and a number of digits of the received
25 unpredictable number.

13. The system of claim 11, wherein the generated data string is electronically transmitted in a data message that further includes a bitmap indicative of formatting of the generated data message.

14. The system of claim 13, wherein the generation module of the
30 computing device is further configured to generate the bitmap based on at least the identified specific formatting template.

15. The system of claim 13, wherein each formatting template of the plurality of formatting templates further includes a bitmap, and

the bitmap included in the data message corresponds to the bitmap included in the identified specific formatting template.

16. The system of claim 11, wherein
the memory further includes, for each of the one or more primary account
5 numbers, a transaction counter, and
the generated data string further includes the transaction counter associated with the specific primary account number.

17. The system of claim 16, wherein the cryptogram is further based on the transaction counter associated with the specific primary account number.

10 18. The system of claim 11, wherein
the generation module of the computing device is further configured to generate a second cryptogram based on at least the unpredictable number and at least one additional algorithm, and
the data string further includes the second cryptogram.

15 19. The system of claim 11, wherein the data string further includes at least one extra digit, and where a number of extra digits is based on the length of the specific primary account number and a number of digits of the received unpredictable number.

20 20. The system of claim 19, wherein the at least one extra digit stores cardholder verification method data.