NIST Interagency Report 7452

National Institute of
Standards and Technology
U.S. Department of Commerce

Secure Biometric Match-on-Card Feasibility Report

David Cooper
Hung Dang
Philip Lee
William MacGregor
Ketan Mehta

NIST Interagency Report 7452

Secure Biometric Match-on-Card Feasibility Report

David Cooper
Hung Dang
Philip Lee
William MacGregor
Ketan Mehta

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

November 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Dr. James Turner, Acting Director

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This Interagency Report discusses ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report, 112 pages

(November 2007)

Acknowledgements

The authors, William MacGregor and David Cooper of the National Institute of Standards and Technology, Ketan Mehta of Mehta Inc., Hung Dang of Booz Allen Hamilton, and Philip Lee of Identity Technology Partners wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors appreciate the many contributions from the product developers and integrators to the weekly teleconferences and the workshop. The authors also acknowledge the important and timely contributions of Gemalto, Oberthur Card Systems, Sagem Morpho Incorporated, and TecSec Incorporated to this study.

Table of Contents

List of Appendices

List of Tables

1. Introduction

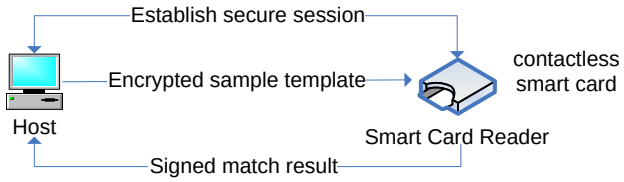
On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12) [1], entitled "*Policy for a Common Identification Standard for Federal Employees and Contractors.*" HSPD-12 required the development and implementation of a government-wide standard for secure and reliable forms of identification for Federal employees and contractors. In response, NIST developed the Federal Information Processing Standard 201 (FIPS 201) [2], *Personal Identity Verification (PIV) of Federal Employees and Contractors*, to establish a standard for identity credentials. NIST also issued several special publications in support of FIPS 201 to enable interoperable implementations.

FIPS 201 and its associated special publications define a method to perform biometric match-off-card authentication of a PIV cardholder when the PIV card is inserted into a contact smart card reader. Today, many smart cards, however, implement match-on-card technologies and are desiged to perform cardholder authentication using contactless interface. Contactless match-on-card operation requires additional security measures to ensure the transaction data is encrypted and can be securely transmitted, which can impact performance. NIST conducted the Secure Biometric Match-on-Card (SBMOC) feasibility study to understand the effects of security on performance. This report describes the tests that were conducted to obtain timing metrics for the SBMOC feasibility study and provides a summary of the test results.

This feasibility study also allows NIST to explore smart card technology advancements for possible extension of the FIPS 201 and / or other smart card standards.

2. Background

In June 2007, NIST extended an open invitation to companies to participate in the SBMOC feasibility study. The purpose of the study was to determine if secure biometric match-on-card operations could be performed in less than 2.5 seconds per transaction.[1] The feasibility study was conducted per guidelines set forth in the NIST Test Approach for SBMOC Feasibility Study (see Appendix D). The test approach describes a Public Key Infrastructure (PKI) based protocol for performing secure biometric match-on-card authentication of a cardholder using contactless operation. The protocol describes general message transactions so that variations in protocol implementation by participants are acceptable so long as the security, functional, and performance objectives defined in Sections 2 and 3 of Appendix D are met. An example use case scenario is as follows:



+ The cardholder presents their card to a contactless biometric reader.
+ The cardholder presents their finger to the biometric scanner.
+ The host establishes a secure session with the card.
+ The host prepares an encrypted template containing the fingerprint (image or minutia) and transmits it via contactless interface to the card.
+ The card decrypts the template and compares it with the reference template stored on the card.
+ The card returns signed result (i.e., Yes/No) to the host.

At the time this study began, NIST was unable to identify any commercial product meeting all of the requirements in Appendix D. Participants worked with NIST to understand the requirements and then developed submissions. Submissions received for the feasibility study that met the stated objectives were tested by NIST. The subsequent sections in this report discuss the test procedures and the results of successful tests obtained from the feasibility study. The results of unsuccessful tests are not reported.

[1] The template generation time (which is live presentation of a fingerprint) is excluded from the time measurement.

3. Test Process

In order to obtain performance timing metrics, a test fixture was developed that implements the secure message protocol for each Device Under Test (DUT) and records the measured transaction times. Test cases executed for the feasibility study were designed to study how matching/non-matching templates, varying minutia counts, and different encryption algorithms impact transaction times. The following subsections describe the test fixture and procedures used for the feasibility study.

3.1 Test Fixture

The test fixture uses the Win32 Smart Card Application Programming Interface (API) library to communicate with DUTs and smart card readers. The library was used to acquire the following time measurements:

+ Average[2] time to establish a secure session
+ Average time to transmit the encrypted biometric data to the DUT and receive a match result
+ Average total time to perform a complete biometric match-on-card transaction

To perform time measurements, the test fixture sends Application Protocol Data Units (APDU) to a DUT using the SCardTransmit command. The time it takes to execute a SCardTransmit command, which is obtained by computing the time difference before and after a call to SCardTransmit, is then recorded to an output file. For APDUs that require multiple calls to SCardTransmit (e.g., GET RESPONSE), the total elapsed time is determined by adding the time to execute each SCardTransmit operation. An example message sequence between a DUT and the test fixture is as follows:

1. The test fixture selects the SBMOC application on the card.
2. The test fixture performs Get Data to read the PKI certificate from the DUT and validates the certificate.
3. The test fixture requests a challenge from the DUT. The DUT responds with a challenge.
4. The text fixture and DUT generate encryption and Message Authentication Code (MAC) session keys, and finish establishing a secure session.
5. The text fixture encrypts biometric data using session key and sends it to the DUT for verification. The DUT responds with the signed match / no-match result.

After running the test fixture, a Comma-Separated Values (CSV) output file is created that contains the measured times for the DUT used in the test. Table 1 lists the data recorded in the output file. A sample test fixture output appears in Appendix C.

Table 1. Test Fixture Output File Fields

Field Name	Description
Date/Time	Date/time that the test run was executed. Recorded as "mm-dd-yyyy HH:MM:SS".

[2] Throughout this report, "average" is the arithmetic mean of the measured values.

Field Name	Description
Run #	Test run number
Reader	Smart card reader description
Card	DUT description
Symmetric Crypto	Name of symmetric cryptographic algorithm used in the test (e.g., “2 Key TDES - CBC”, “AES-128 - CBC”)
Asymmetric Crypto	Name of asymmetric cryptographic algorithm used in the test (e.g., “RSA 1024”, “RSA 2048”)
Fingerprint Filename	Filename of sample fingerprint template used in the test run
Finger	Name of finger associated with the sample fingerprint template. Set to “Unknown finger” if this information is not known.
Minutia Count	Minutia count of the sample fingerprint template
Total Time	Total time to perform the biometric match-on-card operation. This is measured as the time from when the SBMOC application is selected until the time when a result is returned from the DUT, and includes host-processing time to perform cryptographic and other necessary functions. In the above example, Total Time is approximately (1) + (2) + (3) + (4) + (5).
T0	Time to establish a secure session. This time does not include the time to select the SBMOC application. In the above example, T0 = (2) + (3) + (4).
T1	Time to authenticate the biometric data after a secure session has been established. In the above example, T1 = (5).
Cert Verified	Indicates if the X.509 certificate loaded on the DUT has been validated. If the “Perform certificate validation” checkbox is not checked then this field will be set to “N/A”.
Finger Verified	Indicates if the sample biometric data matched the reference biometric data stored on the DUT. Set to either “Yes” or “No”.

3.2 Test Execution

The smart card reader used in the tests was an SCM SDI010 dual interface reader. The reader’s technical specifications are given in Table 2.

Table 2. Smart Card Reader Technical Specifications

Category	Description
Host Interface	• Full speed USB 1.1 (12 Mbps) • High Bus powered device • CCID compliant
Firmware	• Version 7.09

Category	Description
Contactless	• Support of ISO 14443 A and B (13.56 MHz) smart cards • ISO 14443 Part 1 to 4 compliant • Operating distance: 1 cm • Communication speed: up to 848 Kbit/s
API	• PC/SC driver version 5.09

For each test case, a DUT was loaded with a reference fingerprint template containing a minutia count of 41, 34, or 27 in either ANSI 378 or ISO/IEC 19794-2 compact format (depending on the DUT being tested). In addition, each DUT was loaded with an X.509 certificate that was generated using the NIST PIV Data Generator tool. The size of the generated certificates was kept consistent by changing only the public key modulus and exponent associated with each certificate to match the public/private key pair stored on a DUT. For tests using Rivest Shamir Adleman (RSA) 1024, the size of the certificate used was 1,345 bytes and for RSA 2048, the certificate size was 1,477 bytes.

Testing consisted of sending matching and non-matching sample fingerprint templates to a DUT for verification in alternating sequence. First, sample fingerprint templates containing a minutia count of 41 were sent to the DUT for verification and time values were recorded. The process was repeated for sample fingerprint templates containing a minutia count of 34 and 27. Live fingerprint scans were not used in the tests since it was desirable to maintain a controlled test environment where the minutia count of the sample fingerprint templates could be regulated. Instead, the sample fingerprint templates were read from files generated from fingerprint scans beforehand. For each test case, 200 trials were run so that 100 time values could be collected each for matching and non-matching templates.

The DUT was powered continuously during the automated sequence of 200 trials. As a consequence, transaction delays that could result from operations at DUT power-up, for example FIPS 140-2 power-up diagnostic tests, are not visible in the measurements.

Table 3 provides a summary of the DUTs used in the feasibility study. Multiple DUTs may correspond to the same physical card but have been given unique names to differentiate the test configurations. Note that the DUTs submitted are prototypes constructed to meet the requirements stated in Appendix D. In conformance with the "no endorsement" policy of NIST, the participants' DUT names have been omitted.

Table 3. DUT Summary

DUT Name	Crypto Mechanism	Description
Card 1 (x)	2TDEA, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 2 (x)	AES-128, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 3 (41)	2TDEA, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a proprietary extension and a minutia count of 41.
Card 4 (41)	AES-128, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a proprietary extension and a minutia count of 41.

DUT Name	Crypto Mechanism	Description
Card 5 (x)	2TDEA, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 6 (x)	2TDEA, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 7 (x)	2TDEA, RSA 1024	DUT loaded with ANSI 378 reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 8 (x)	2TDEA, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 9 (x)	3TDEA, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 10 (x)	AES-128, RSA 1024	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 11 (x)	2TDEA, RSA 2048	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 12 (x)	AES-128, RSA 2048	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 13 (41)	2TDEA, RSA 2048	DUT loaded with ISO 19794-2 compact reference template containing a proprietary extension and a minutia count of 41.
Card 14 (41)	AES-128, RSA 2048	DUT loaded with ISO 19794-2 compact reference template containing a proprietary extension and a minutia count of 41.
Card 15 (x)	2TDEA, RSA 2048	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 16 (x)	2TDEA, RSA 2048	DUT loaded with ISO 19794-2 compact reference template containing a minutia count of 'x', where x = 41, 34, or 27.
Card 17 (x)	2TDEA, RSA 2048	DUT loaded with ANSI 378 reference template containing a minutia count of 'x', where x = 41, 34, or 27.

4. Results

Timing metrics obtained with the test fixture could not be validated with a protocol analyzer since one could not be acquired within the SBMOC test framework that supports the high-speed data rates used by the SCM SDI010 reader. However, the test fixure was built on a test framework for a previous NIST study in which timing metrics were obtained and validated with a protocol analyzer. Hence, there is a reasonable degree of confidence that the timing metrics reported in this document are accurate.

Appendix A contains the average response times for each DUT, separated by matching and non-matching results as well as minutia count. In the charts, "SMC" stands for "Sample Minutia Count" and refers to the minutia count of the sample fingerprint templates sent to the DUT. The average response time is an aggregate of three time values: T0, T1, and Host Processing.

+ T0—refers to the time it took to establish a secure session with the DUT.
+ T1—refers to the time it took to send an encrypted template to the DUT for verification and receive a response.
+ Host Processing—refers to the time spent performing processing on the host-side (e.g., cryptographic functions).

Figure 1 below shows the average response times for all DUTs that support RSA 1024. Figure 2 shows the average response times for all DUTs that support RSA 2048.

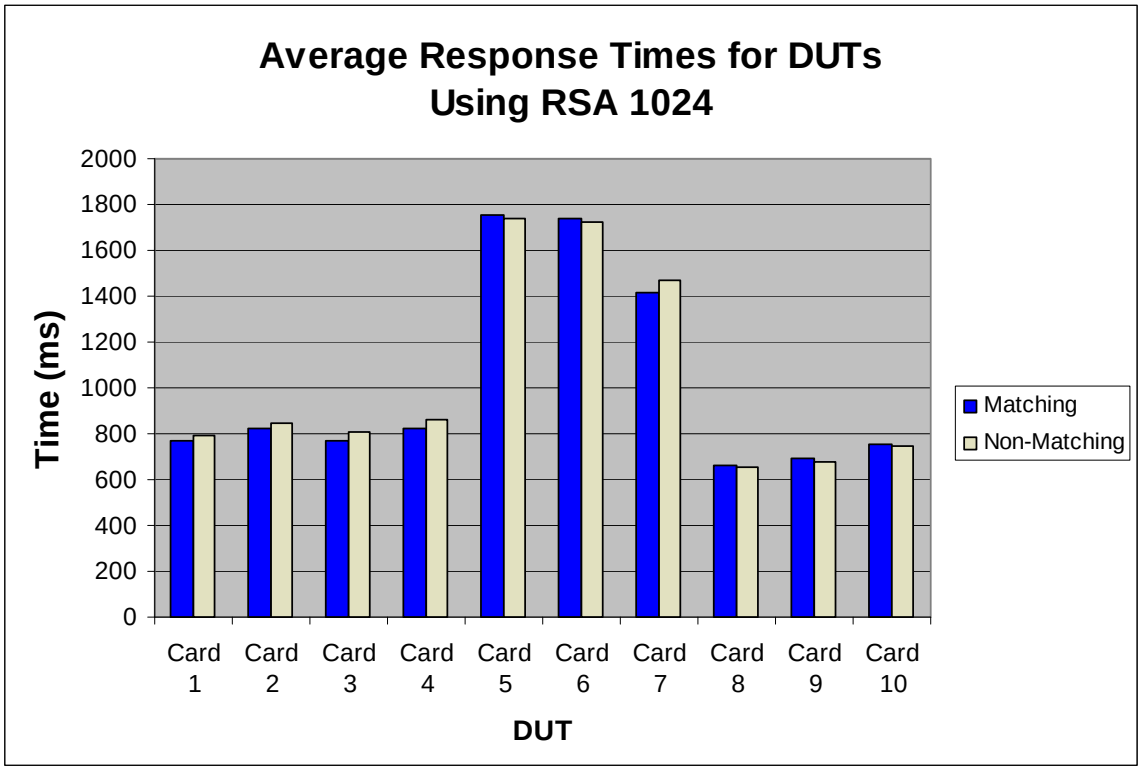


Figure 1. Average Response Times of DUTs Using RSA 1024

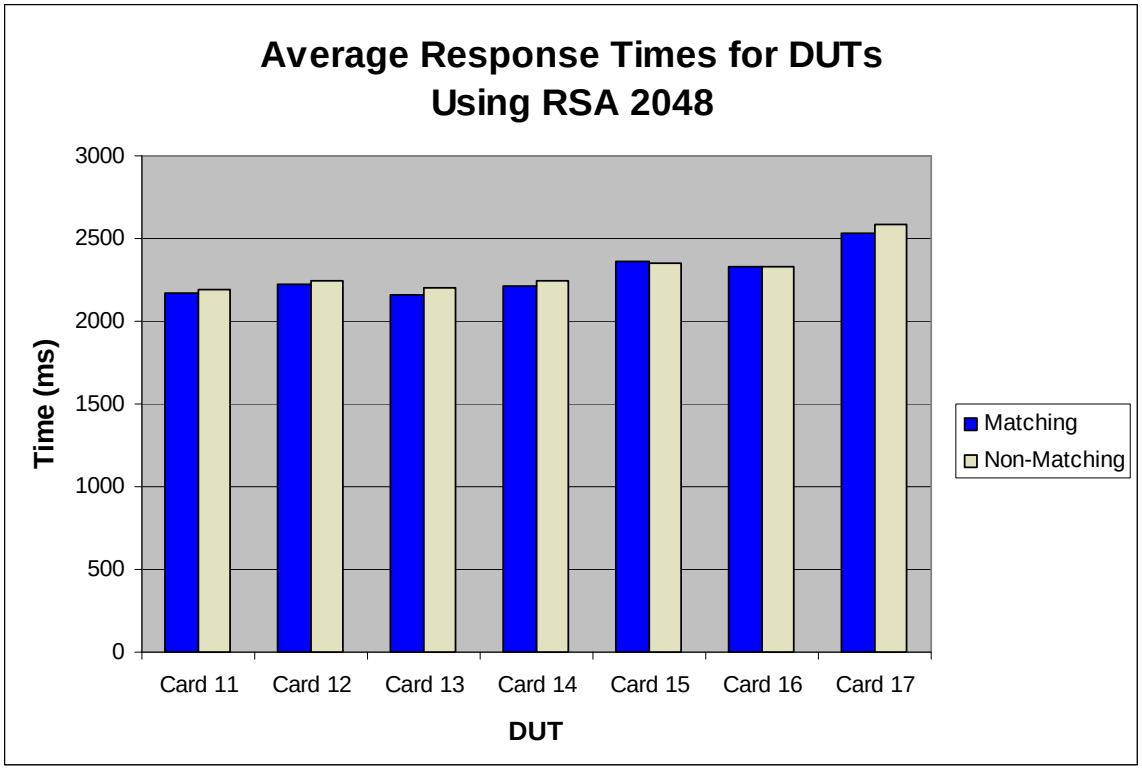


Figure 2. Average Response Times of DUTs Using RSA 2048

Appendix B contains graphs of the response times for each DUT, separated by matching and non-matching results as well as minutia count. A 17 ms fluctuation is visible in the response time charts, e.g., in Figure C-1. This fluctuation can be attributed to the Windows NT clock resolution of the host PC, which is 1/60 second or 17 ms. Such fluctuations are recorded whenever a fixed duration phenomenon is measured repeatedly, starting at random points with respect to a clock tick. Assuming the DUT response time is fixed, the actual DUT response time is approximately the computed average response time, as reported in Appendix A. Whether the assumption holds or not, a 17 ms fluctuation is less than 3% of the measured values in all cases.

In some cases, one or more of the following anomalies were observed while obtaining timing metrics for a DUT:

+ The entire protocol sequence could not be executed (e.g., a secure session could not be established with the DUT). Hence, some graphs may have less than 100 time values for matching and/or non-matching results (an example appears in Figure C-29).

+ A matching template was sent to a DUT for verification and the DUT responded with a "No match" result. Consequently, there may be more non-matching than matching time values (an example appears in Figures C-35 and C-36).

+ Anomalous time values were observed that exceed the 17 ms host clock resolution (an example appears in Figure C-29).

These anomalies may have been caused by a number of different factors, such as Radio Frequency (RF) noise between the DUT and smart card reader, and the actual negotiated operating speed of the DUT.

5. Conclusion

The timing metrics obtained from the SBMOC feasibility study showed that it is possible to securely perform biometric match-on-card operations over the contactless interface of a smart card within 2.5 seconds, while meeting the constraints in Appendix D except the accuracy constraint. The study also showed that the amount of time required to complete an SBMOC operation is dependent on a number of factors, such as the cryptographic mechanisms used, the minutia count of the reference and sample fingerprint templates, and the format of the fingerprint templates.

Accuracy testing of ISO/IEC 19794-2 devices is in progress at this time. Partial results indicate that some devices exhibit accuracy approaching that measured for Minutiae Interoperability Exchange Test (MINEX) 04 implementations, and are likely to exceed the PIV accuracy requirements in Special Publication (SP) 800-76-1. Results will be announced at http://fingerprint.nist.gov/minexII/.

The feasibility study participants informed us that some of the DUTs were constructed by adding firmware and data to PIV card stock that had passed NIST NPIVP and FIPS 140-2 testing. These remarks are further evidence that SBMOC is technically feasible through firmware extensions to existing smart cards.

Appendix A—Average Response Time Charts

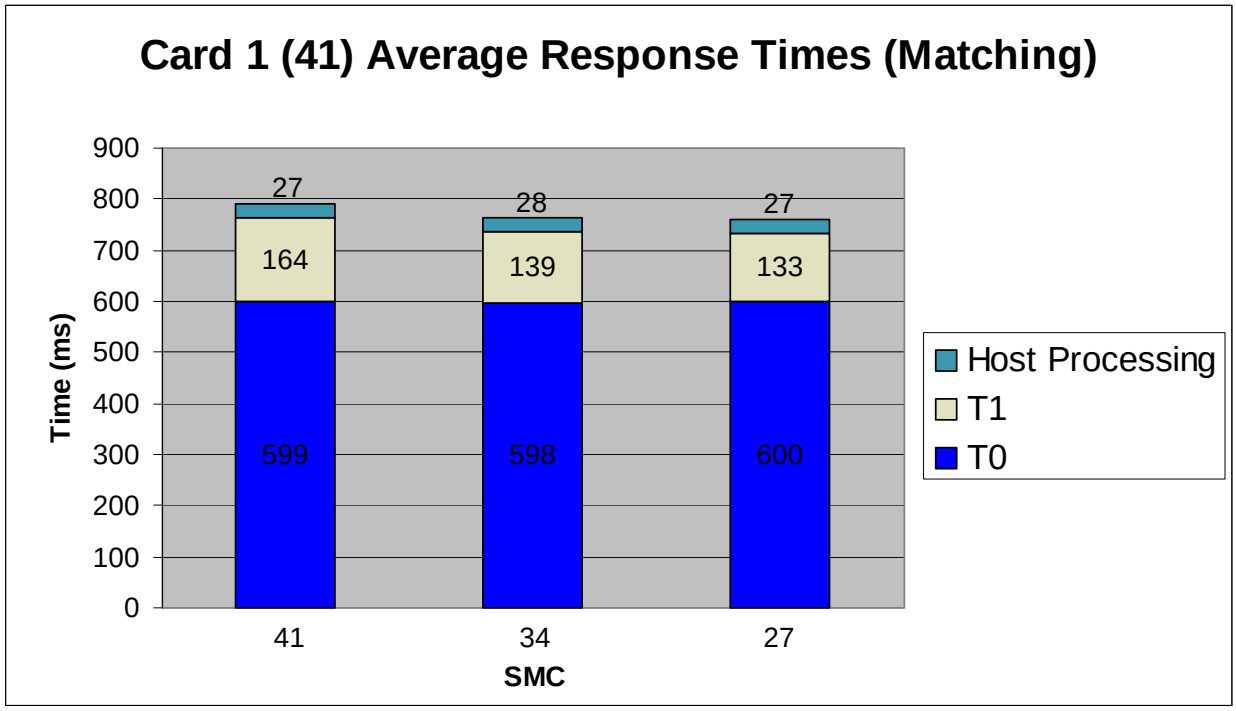


Figure B-1. Card 1 (41) Average Response Times for Matching Templates

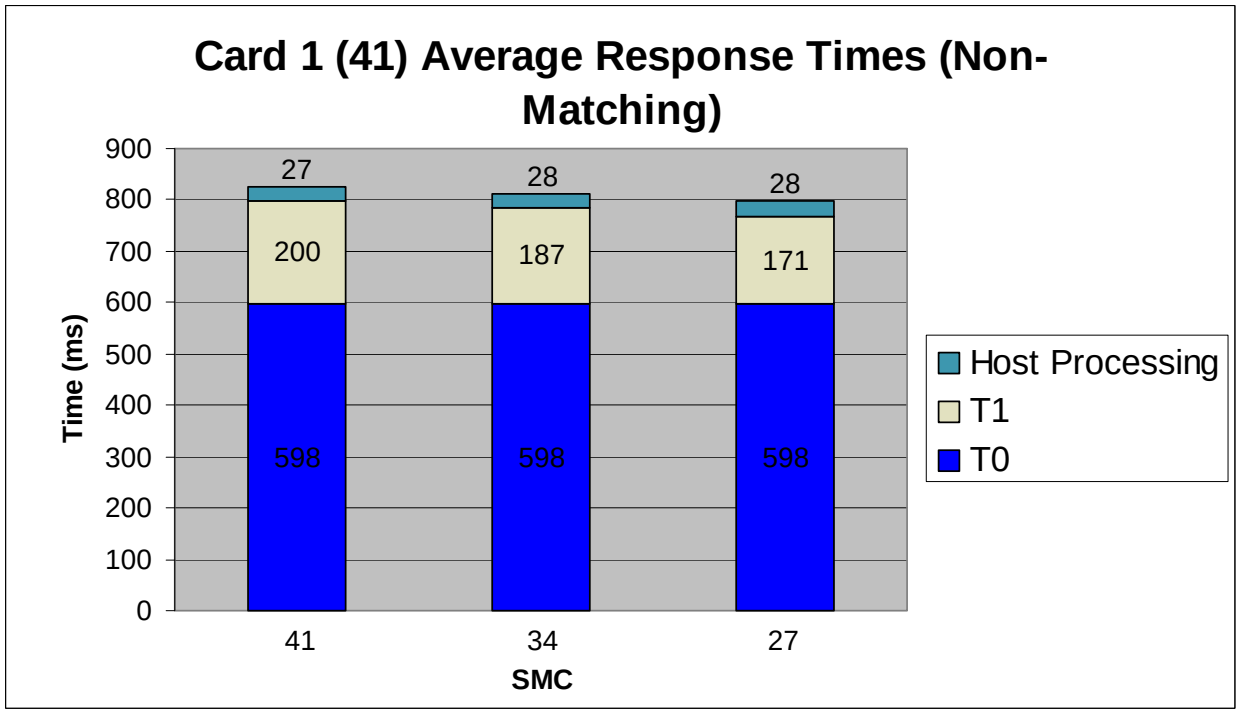


Figure B-2. Card 1 (41) Average Response Times for Non-Matching Templates

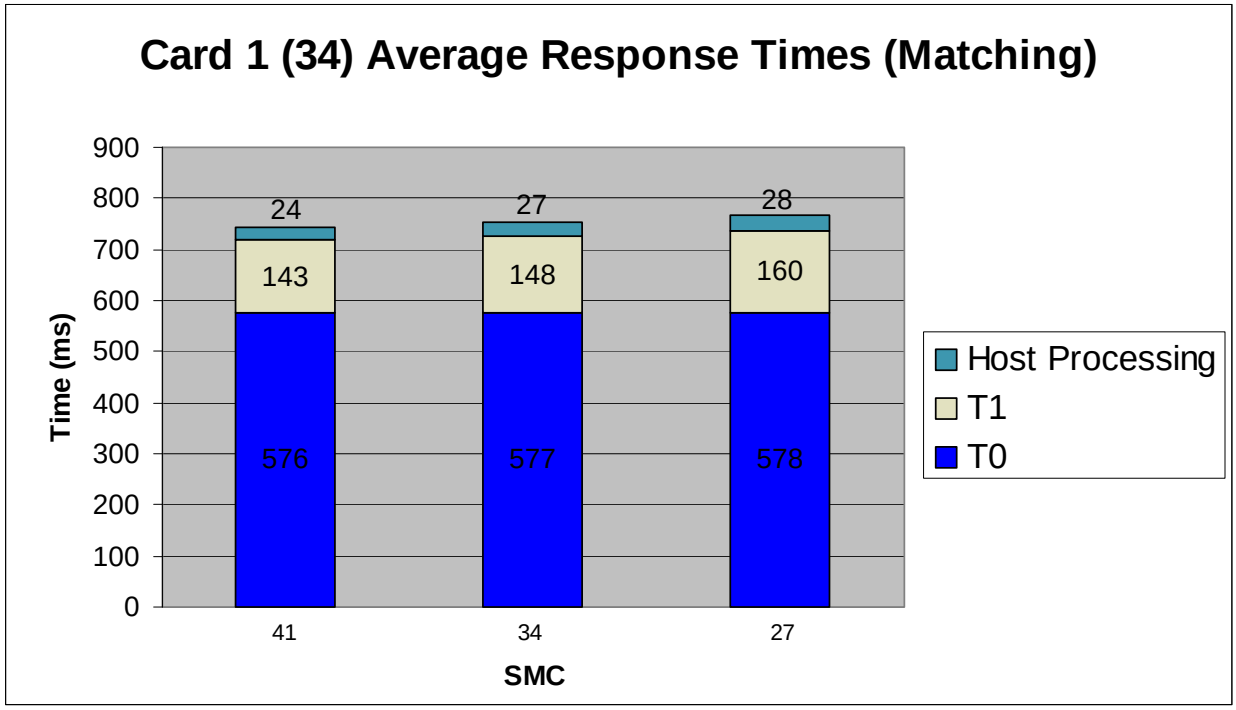


Figure B-3. Card 1 (34) Average Response Times for Matching Templates

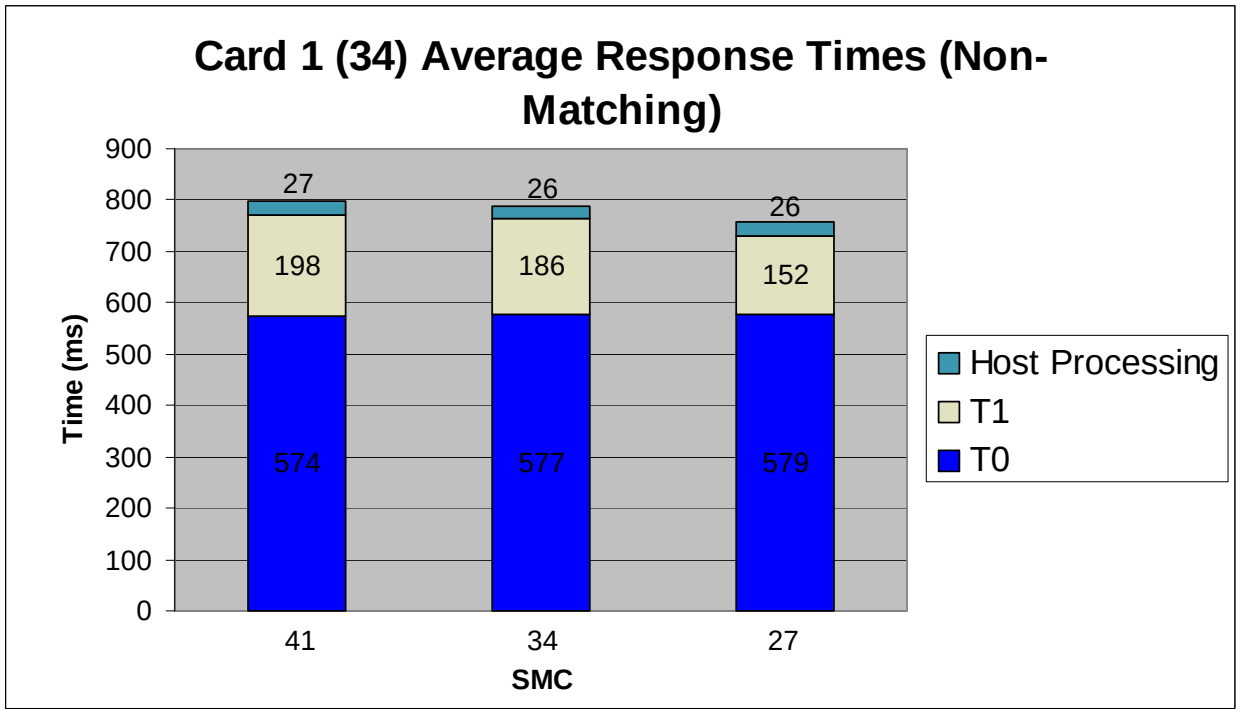


Figure B-4. Card 1 (34) Average Response Times for Non-Matching Templates

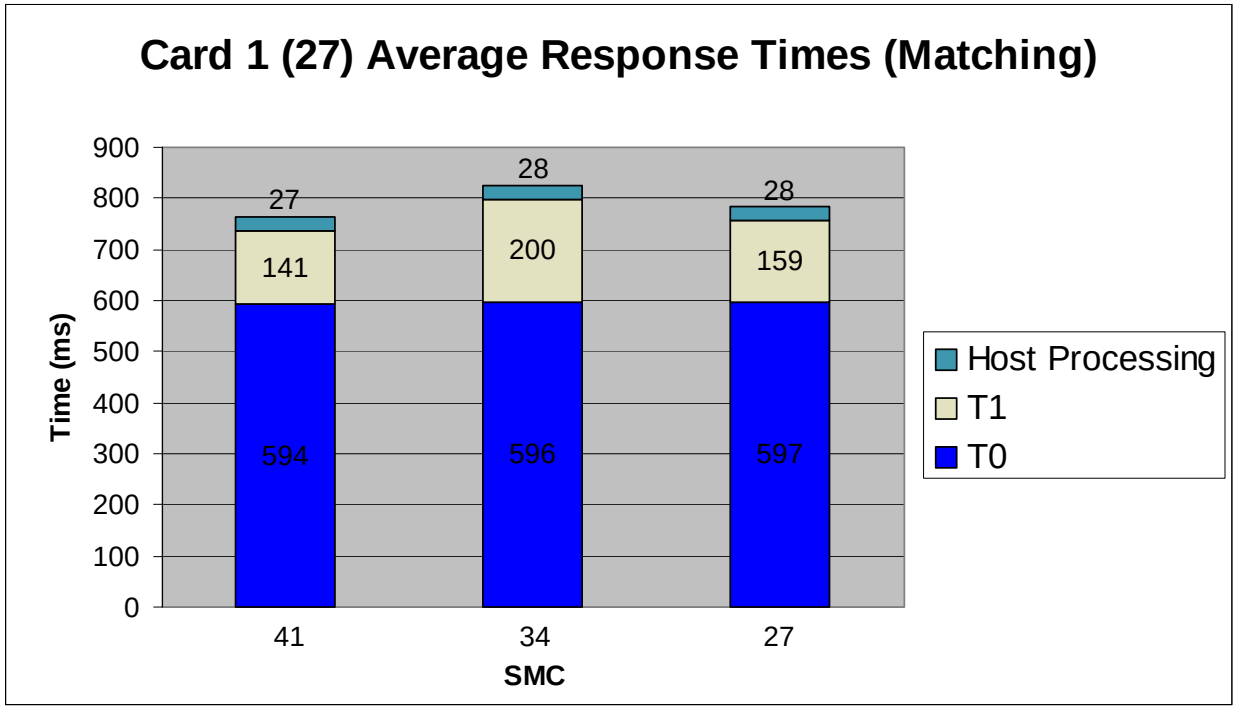


Figure B-5. Card 1 (27) Average Response Times for Matching Templates

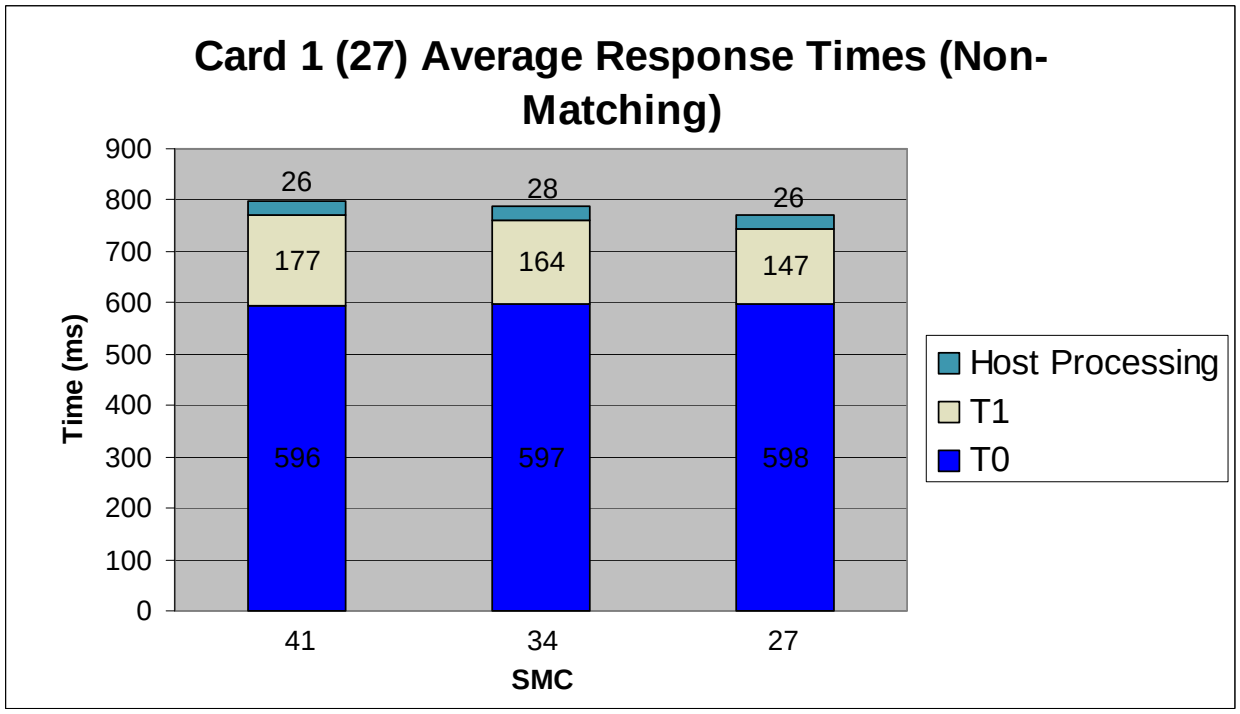


Figure B-6. Card 1 (27) Average Response Times for Non-Matching Templates

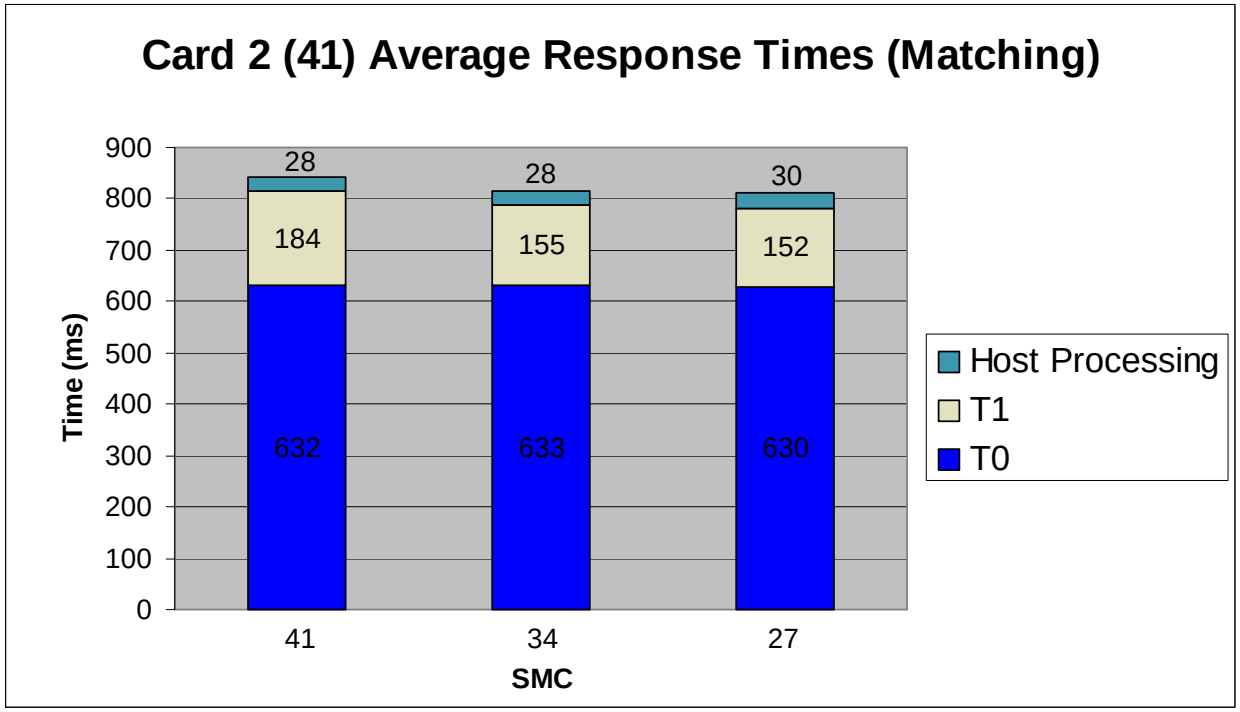


Figure B-7. Card 2 (41) Average Response Times for Matching Templates

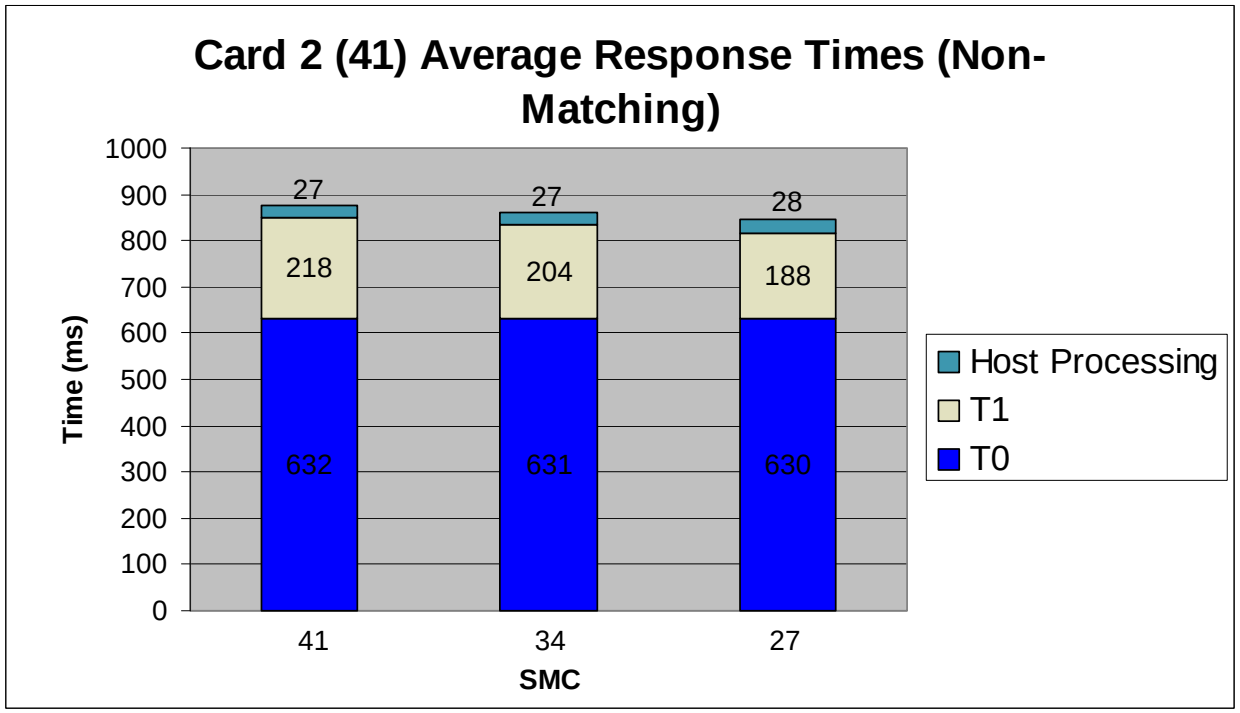


Figure B-8. Card 2 (41) Average Response Times for Non-Matching Templates

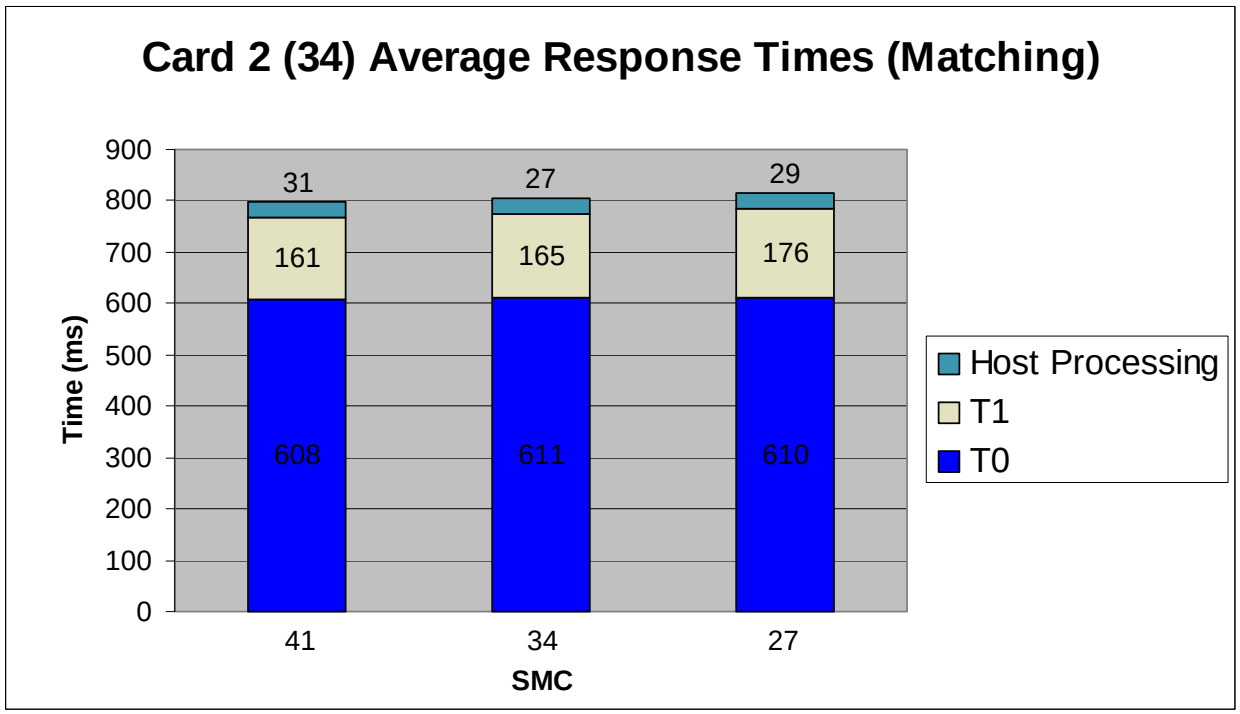


Figure B-9. Card 2 (34) Average Response Times for Matching Templates

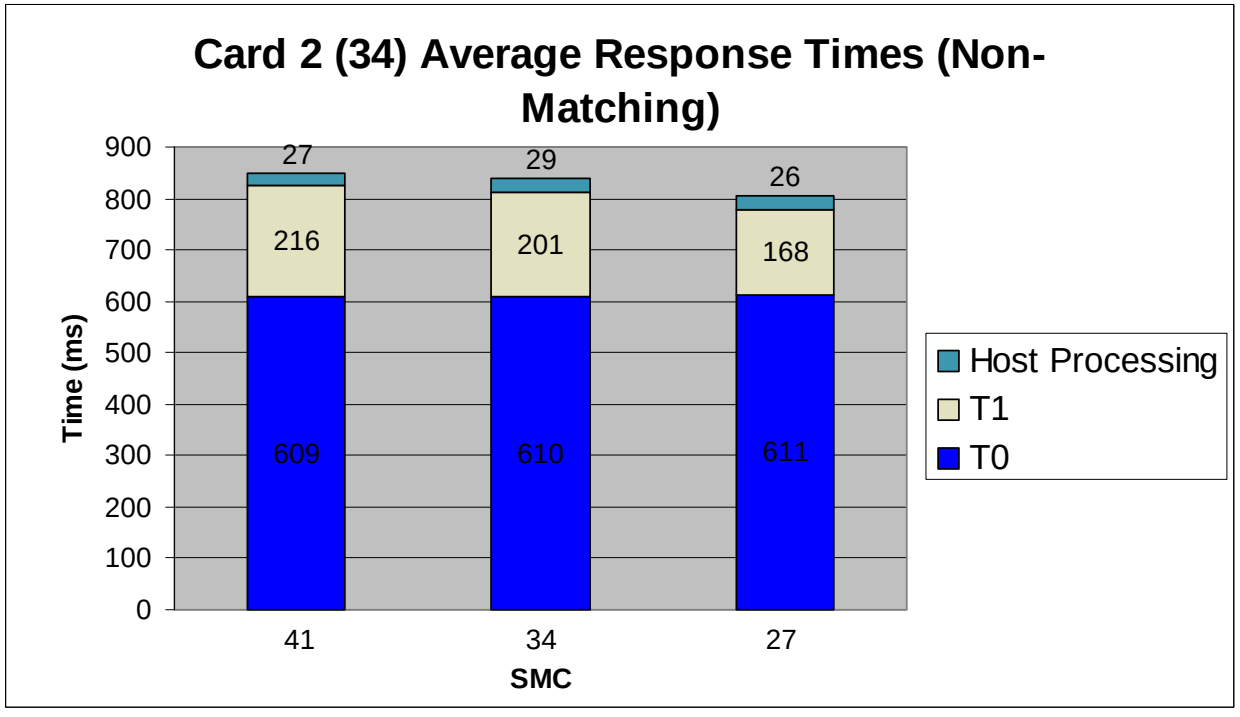


Figure B-10. Card 2 (34) Average Response Times for Non-Matching Templates

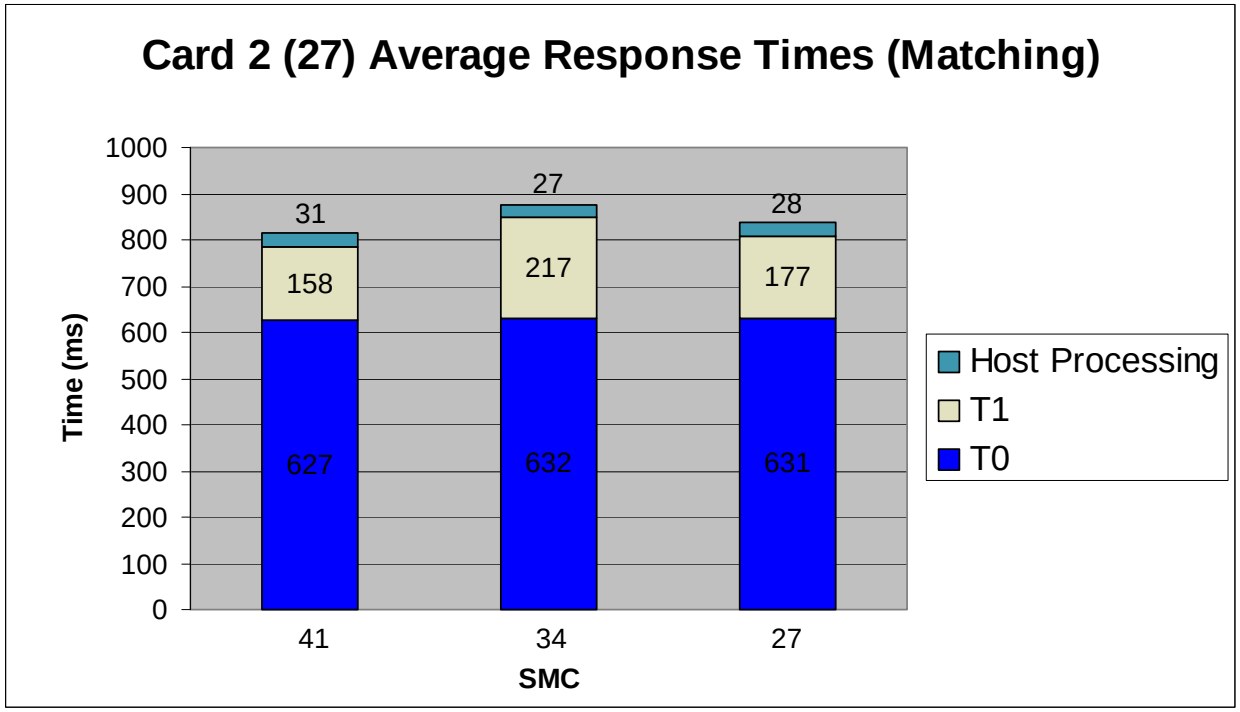


Figure B-11. Card 2 (27) Average Response Times for Matching Templates

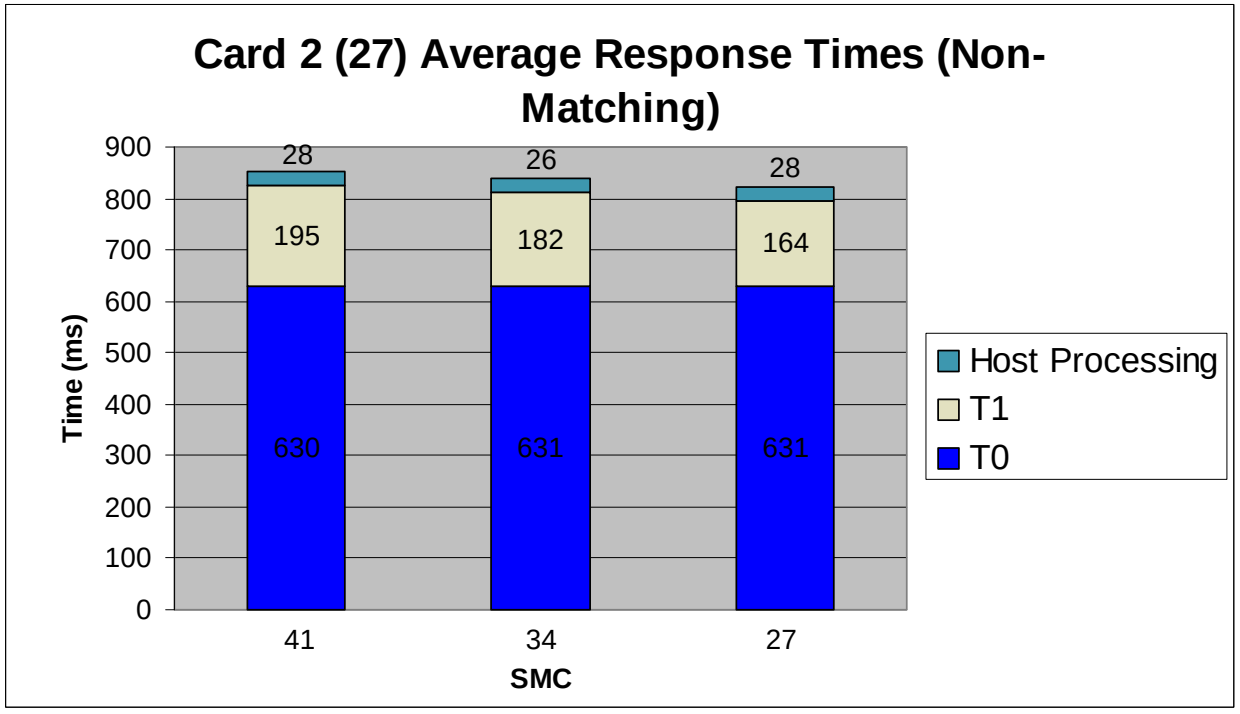


Figure B-12. Card 2 (27) Average Response Times for Non-Matching Templates

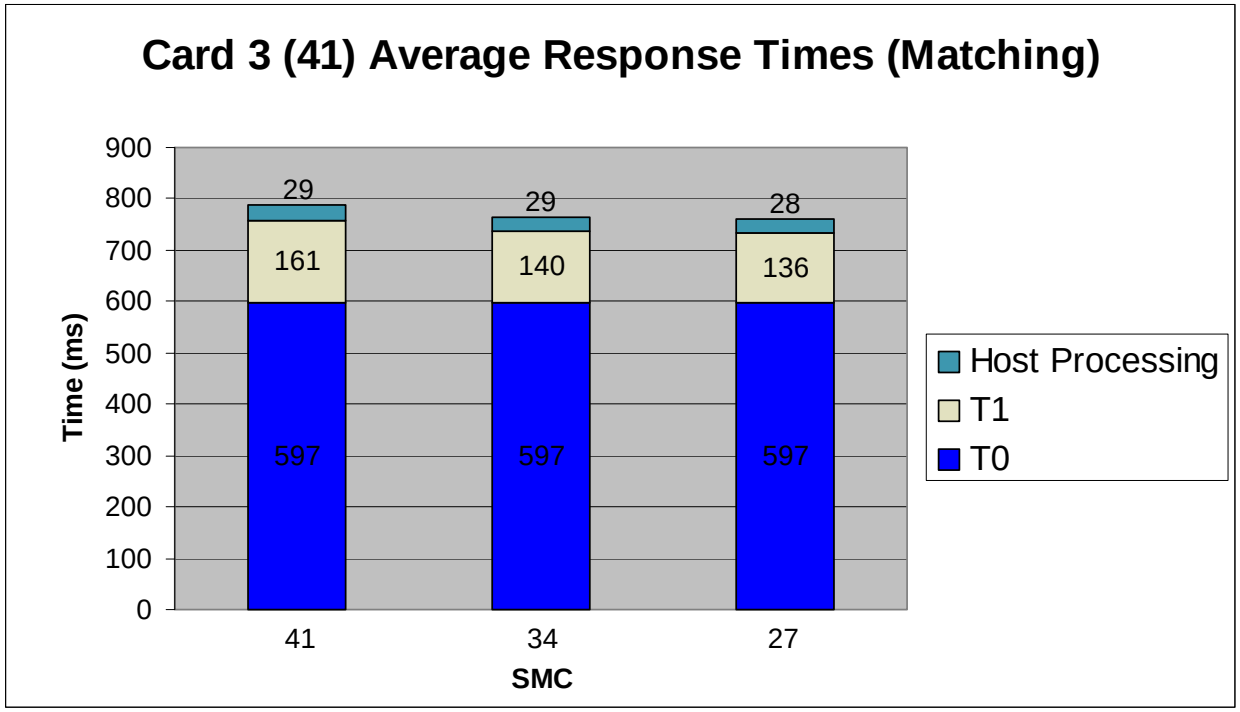


Figure B-13. Card 3 (41) Average Response Times for Matching Templates[3]

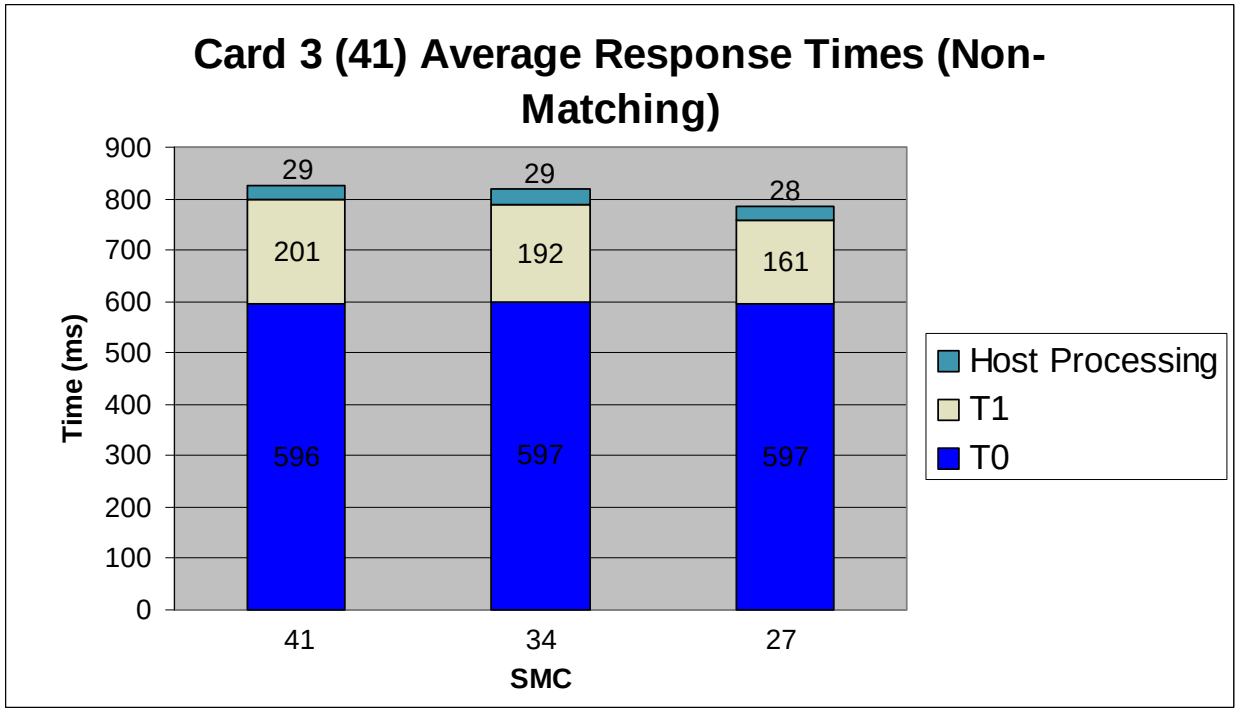


Figure B-14. Card 3 (41) Average Response Times for Non-Matching Templates

[3] Card 3 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

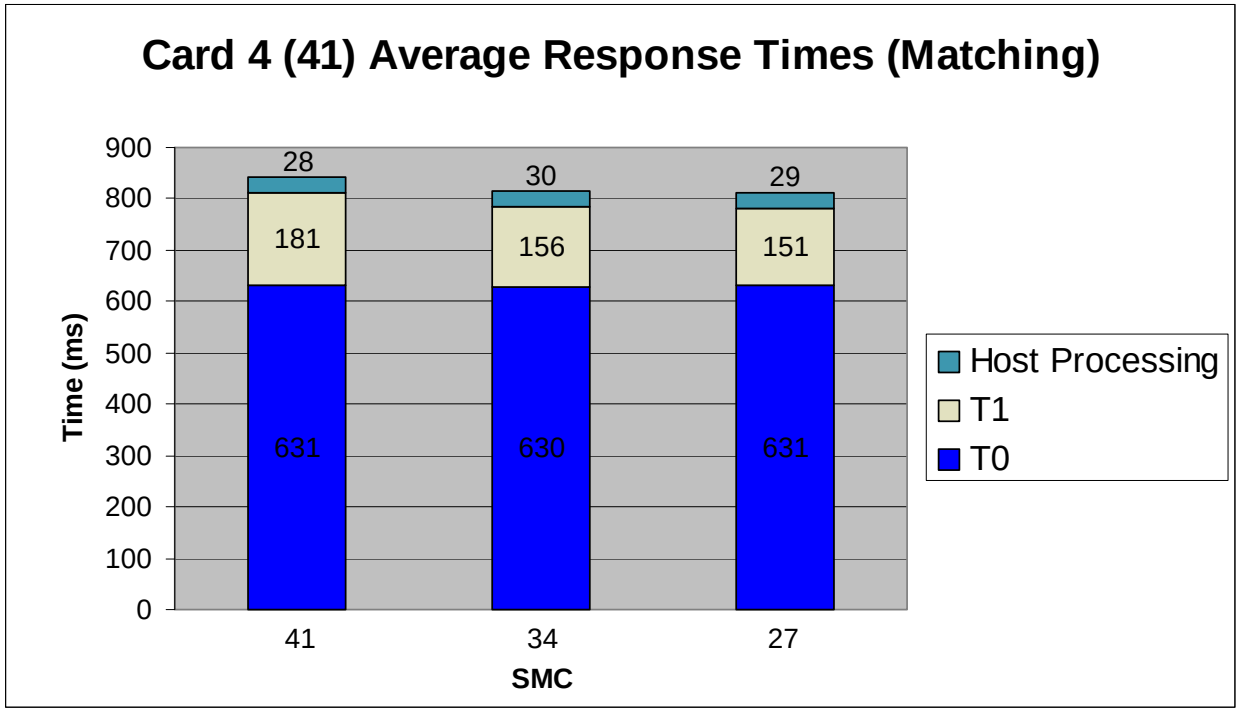


Figure B-15. Card 4 (41) Average Response Times for Matching Templates[4]

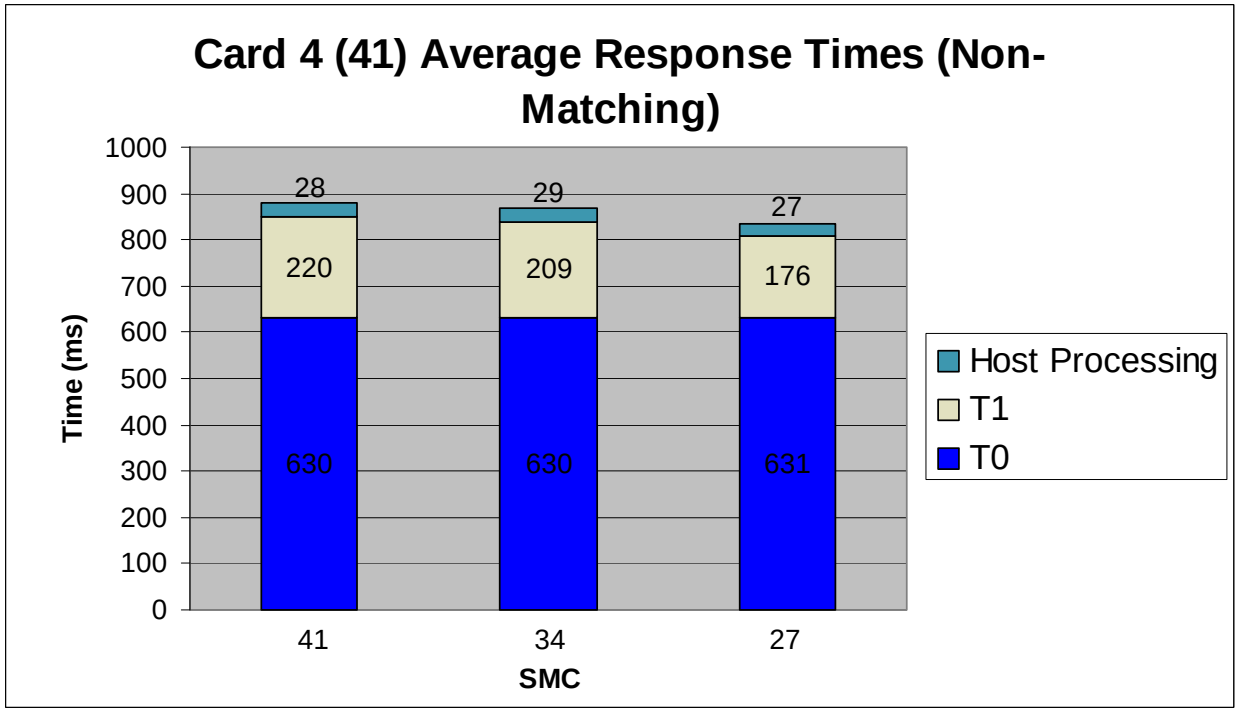


Figure B-16. Card 4 (41) Average Response Times for Non-Matching Templates

[4] Card 4 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

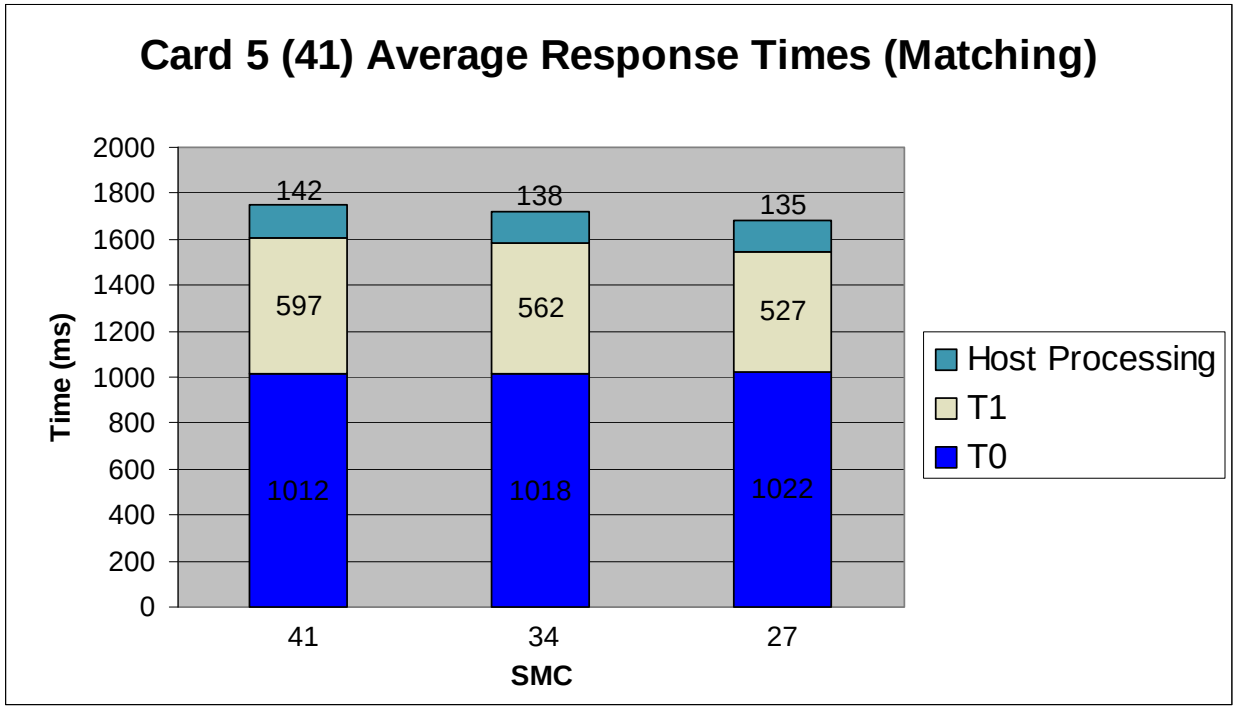


Figure B-17. Card 5 (41) Average Response Times for Matching Templates

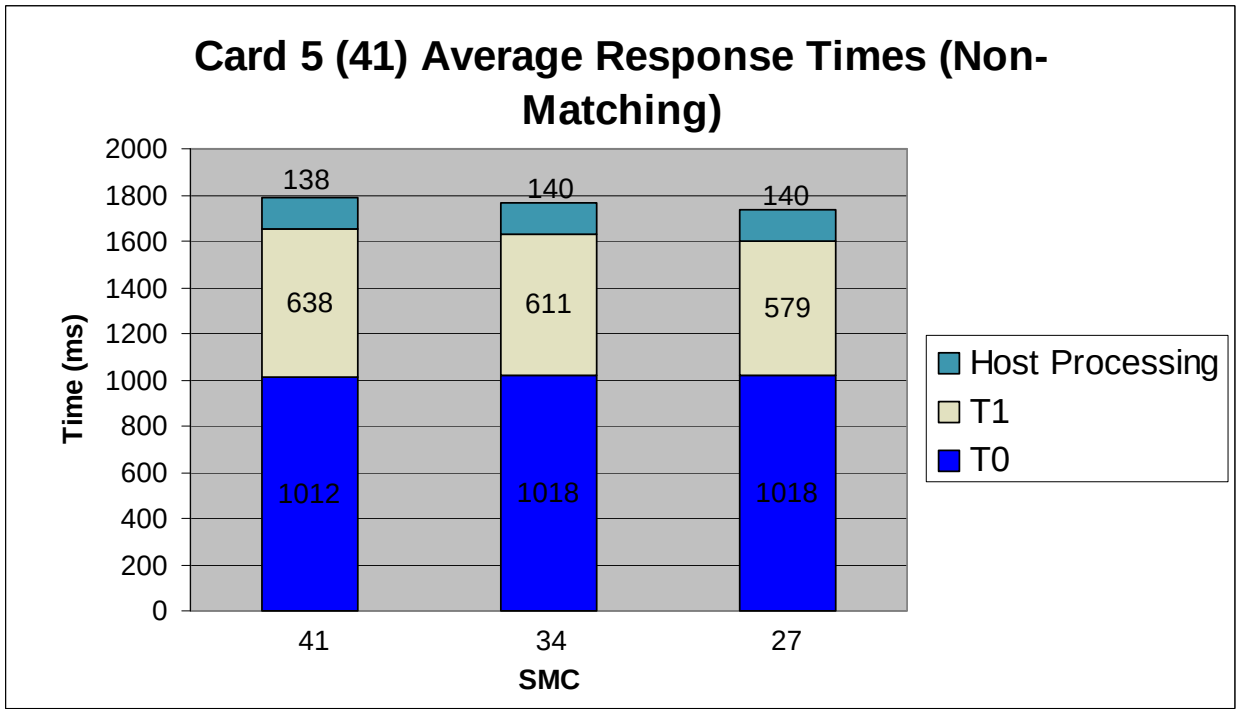


Figure B-18. Card 5 (41) Average Response Times for Non-Matching Templates

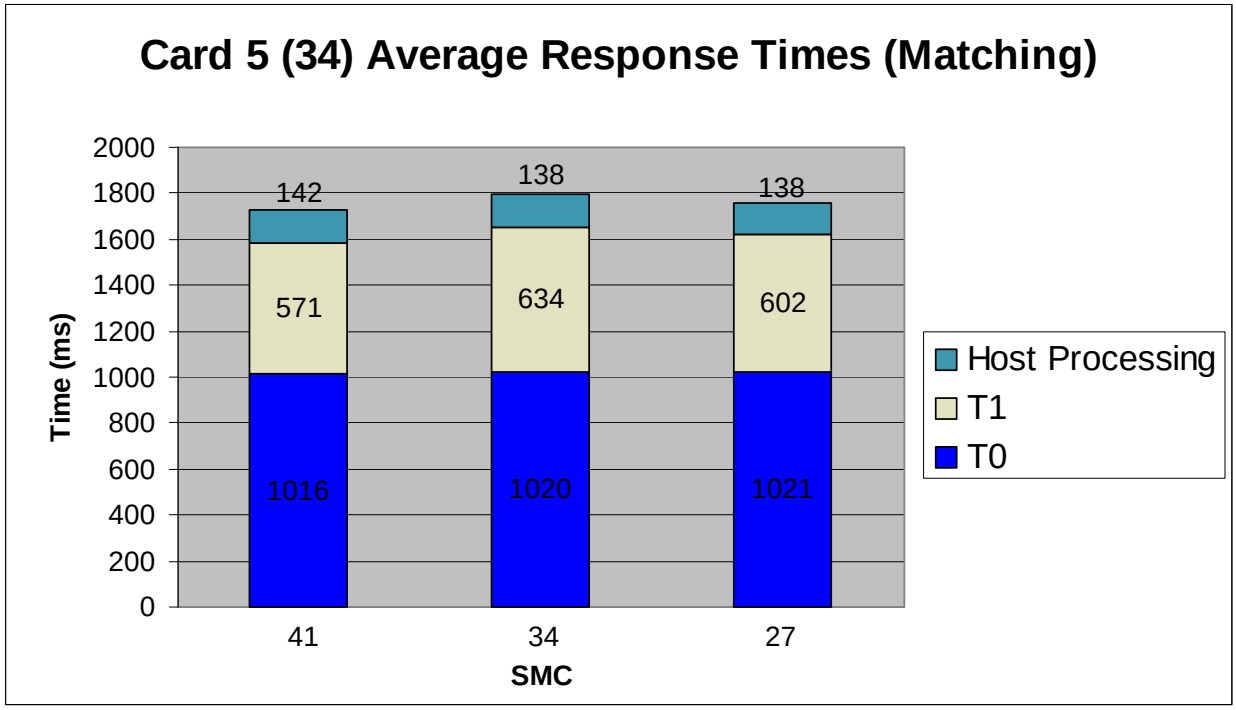


Figure B-19. Card 5 (34) Average Response Times for Matching Templates

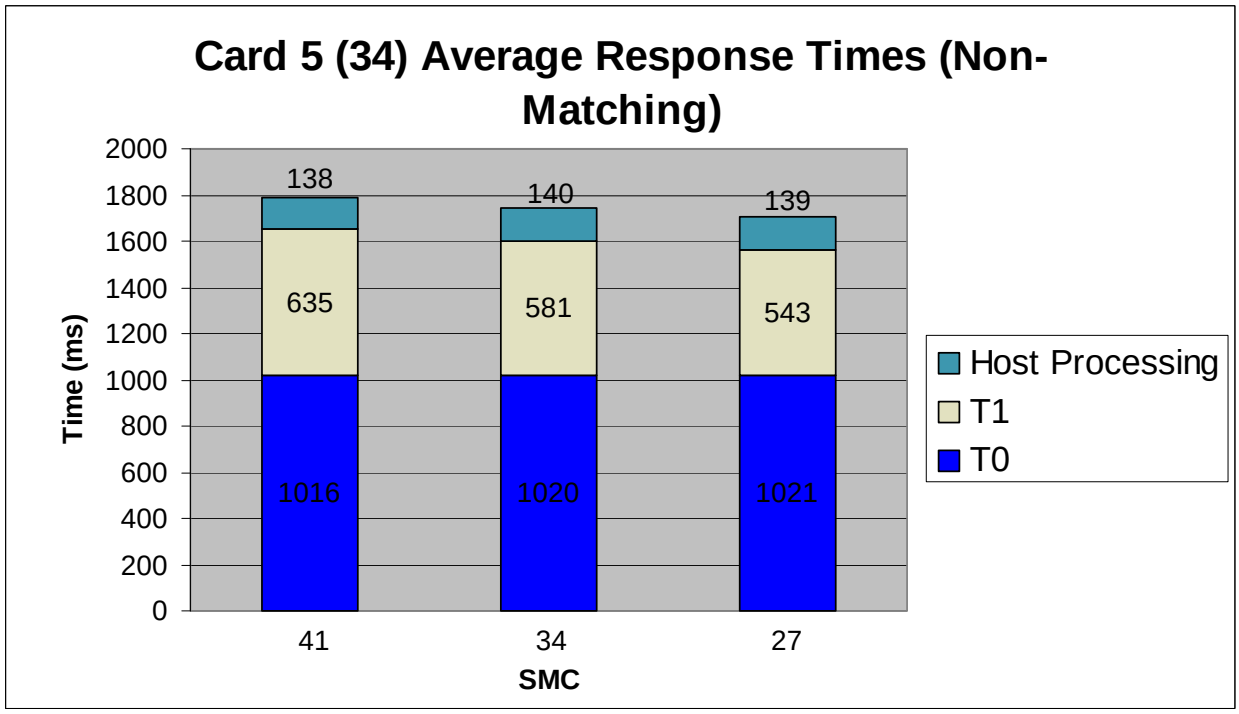


Figure B-20. Card 5 (34) Average Response Times for Non-Matching Templates

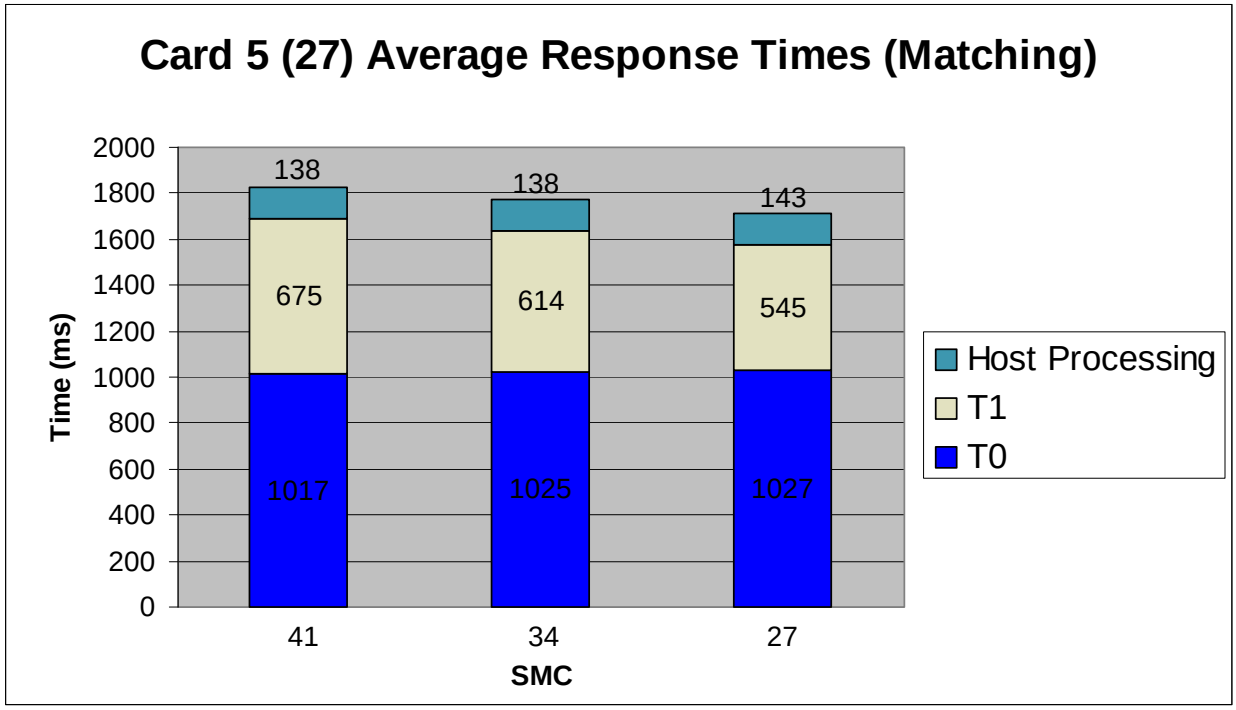


Figure B-21. Card 5 (27) Average Response Times for Matching Templates

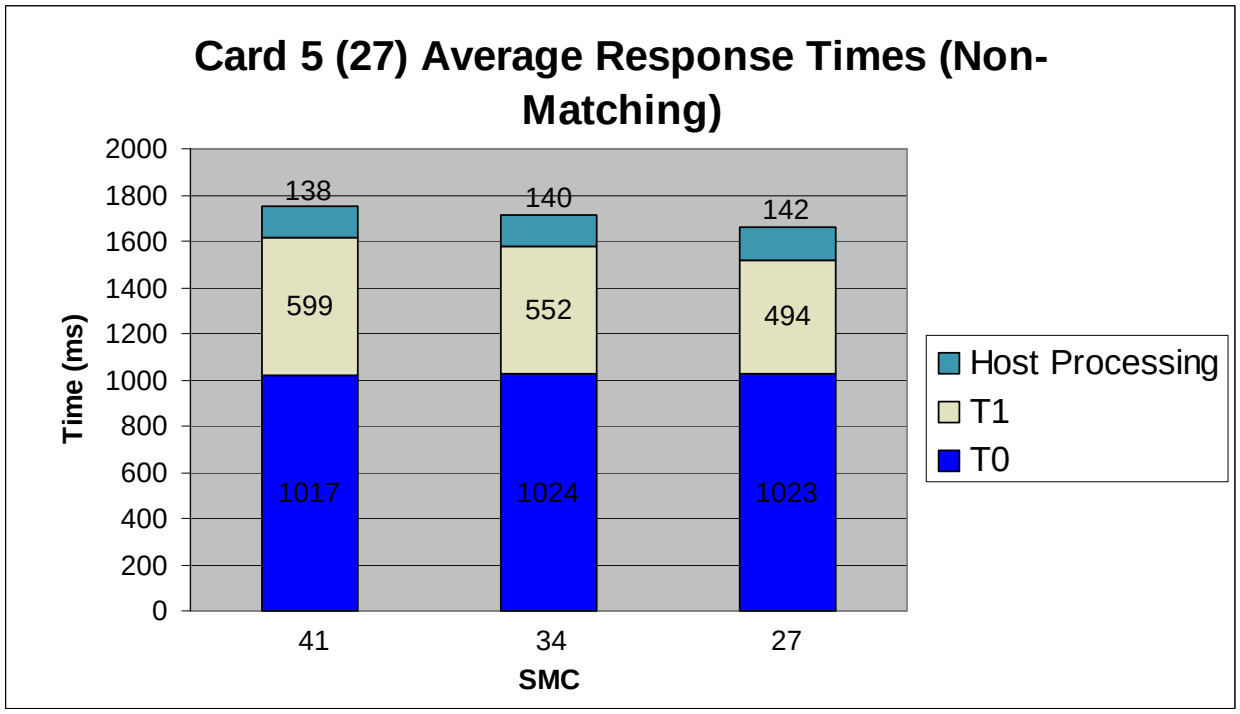


Figure B-22. Card 5 (27) Average Response Times for Non-Matching Templates

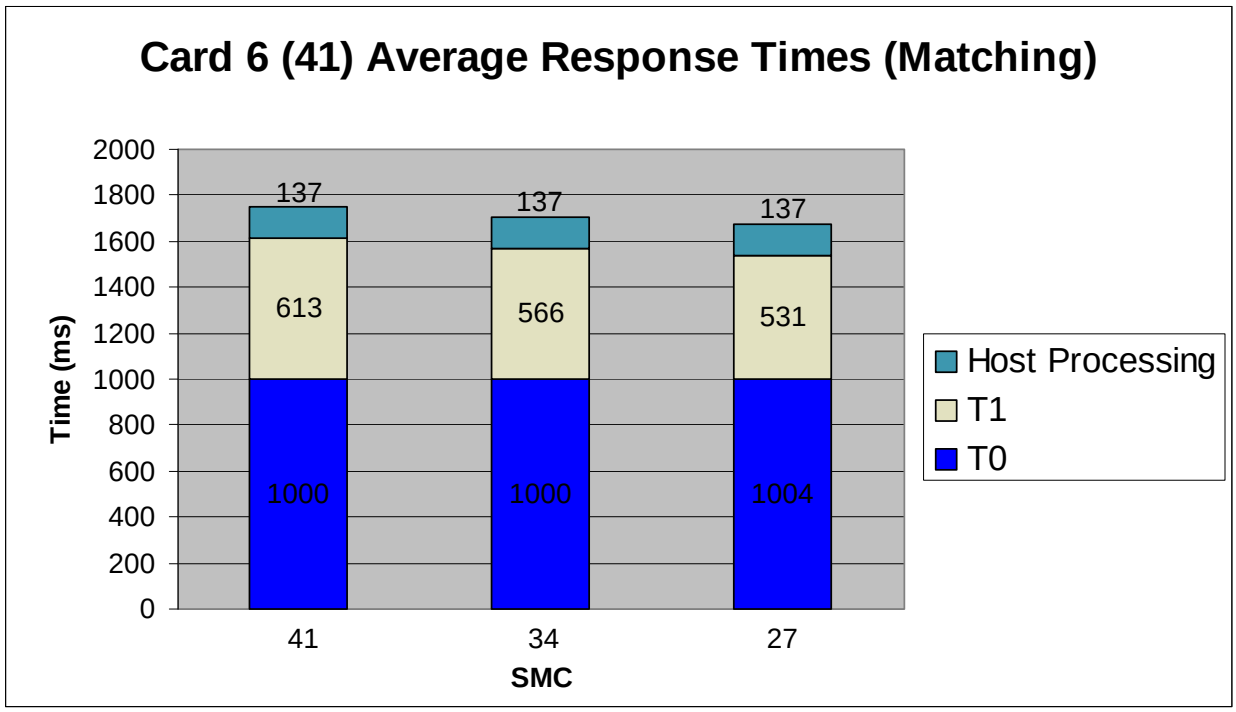


Figure B-23. Card 6 (41) Average Response Times for Matching Templates

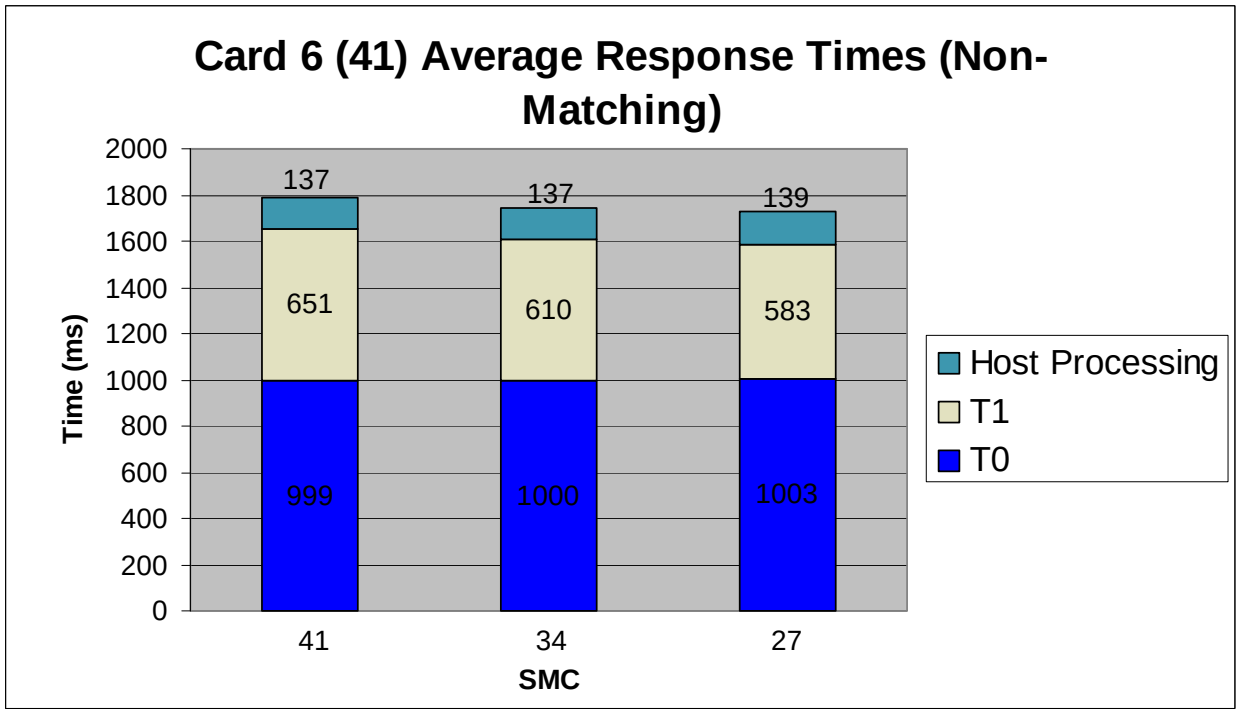


Figure B-24. Card 6 (41) Average Response Times for Non-Matching Templates

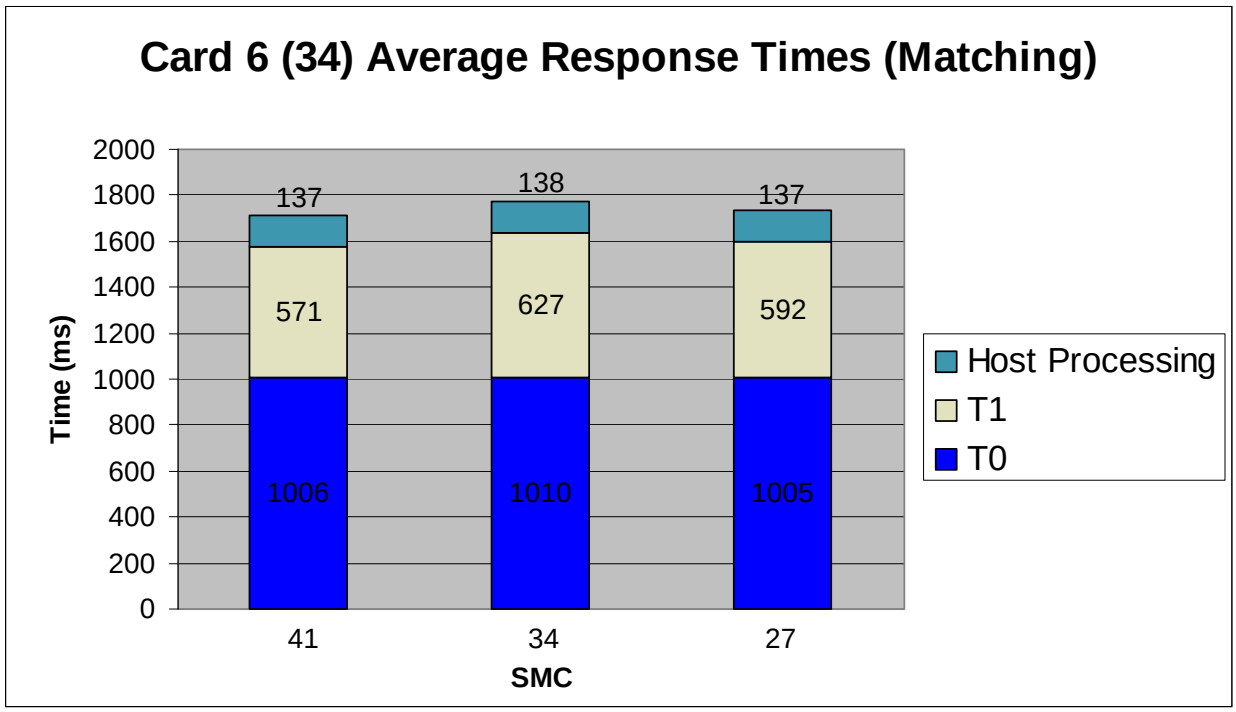


Figure B-25. Card 6 (34) Average Response Times for Matching Templates

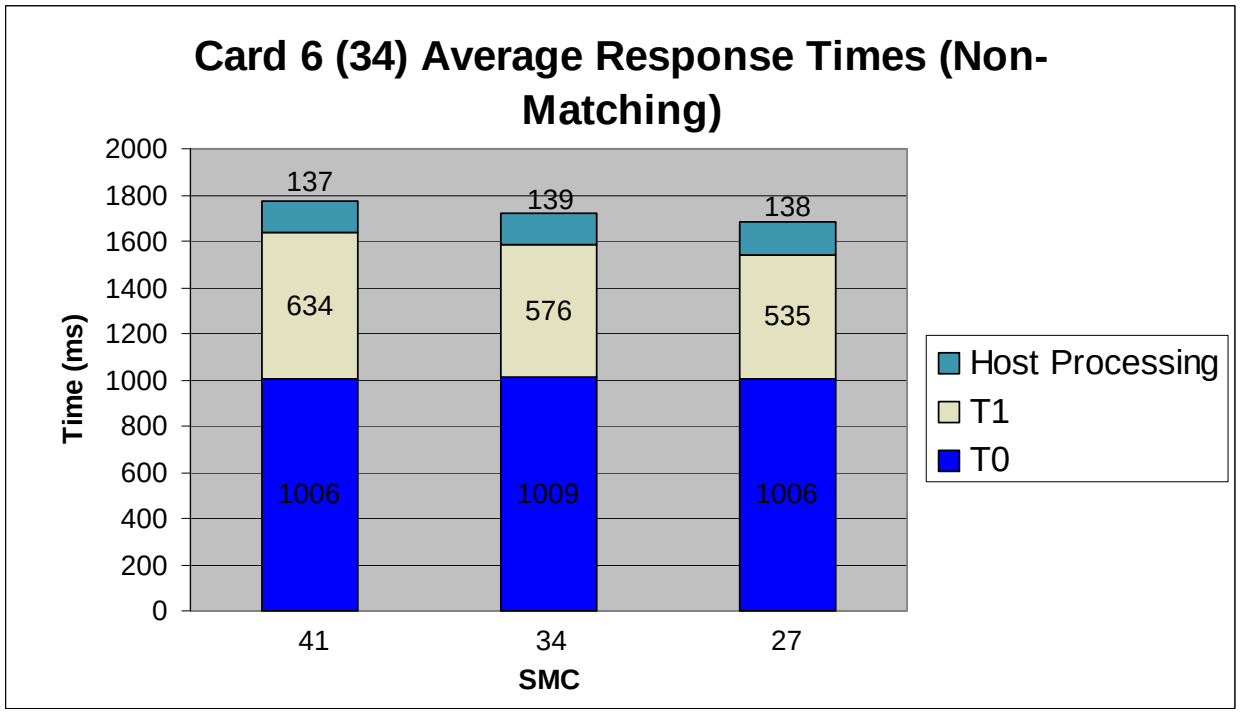


Figure B-26. Card 6 (34) Average Response Times for Non-Matching Templates

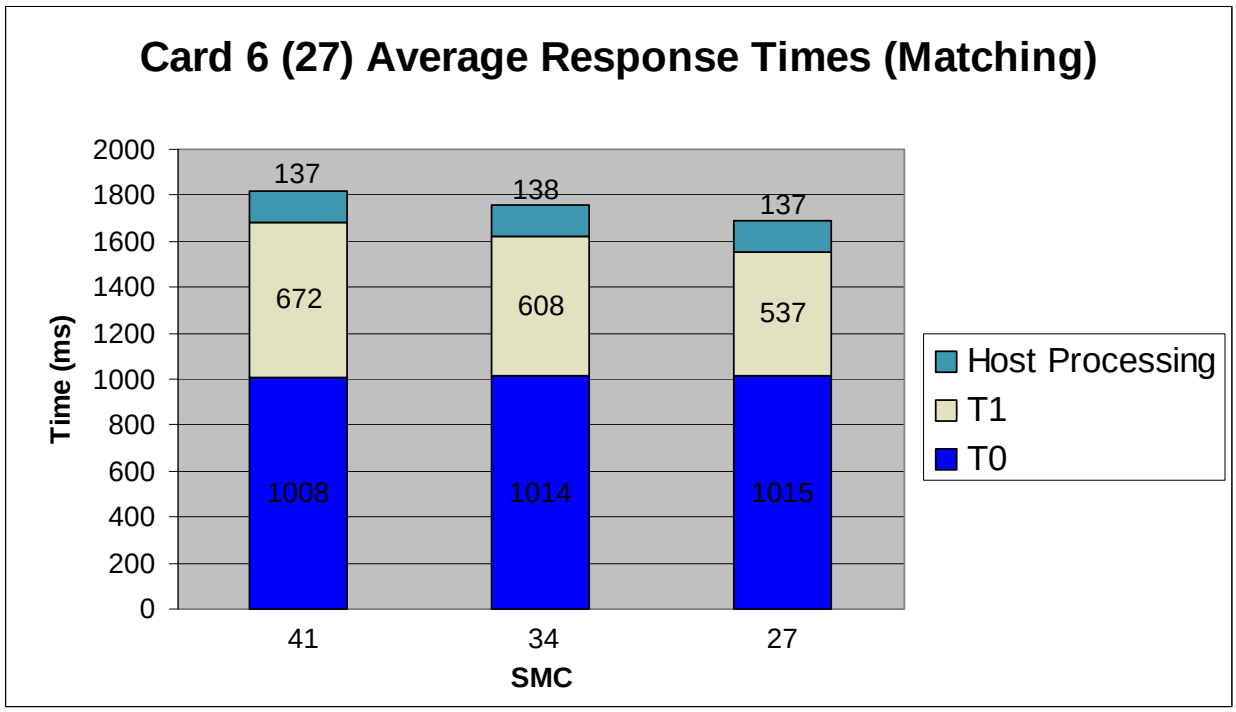


Figure B-27. Card 6 (27) Average Response Times for Matching Templates

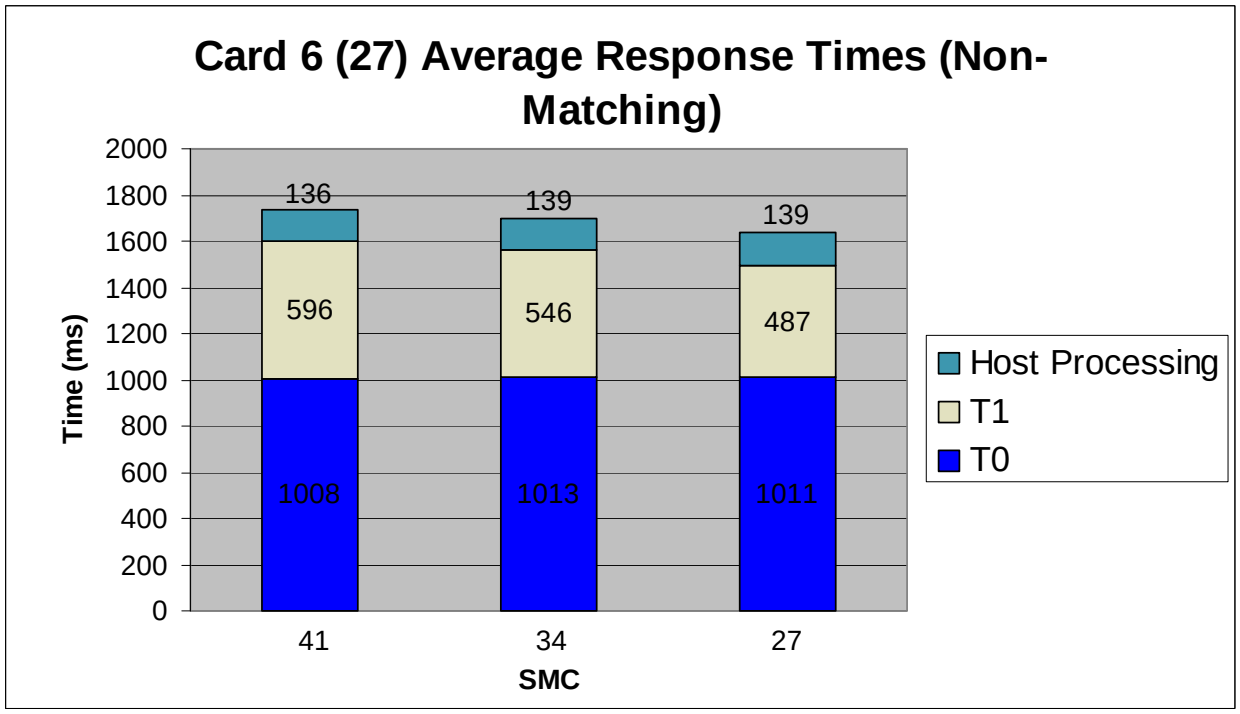


Figure B-28. Card 6 (27) Average Response Times for Non-Matching Templates

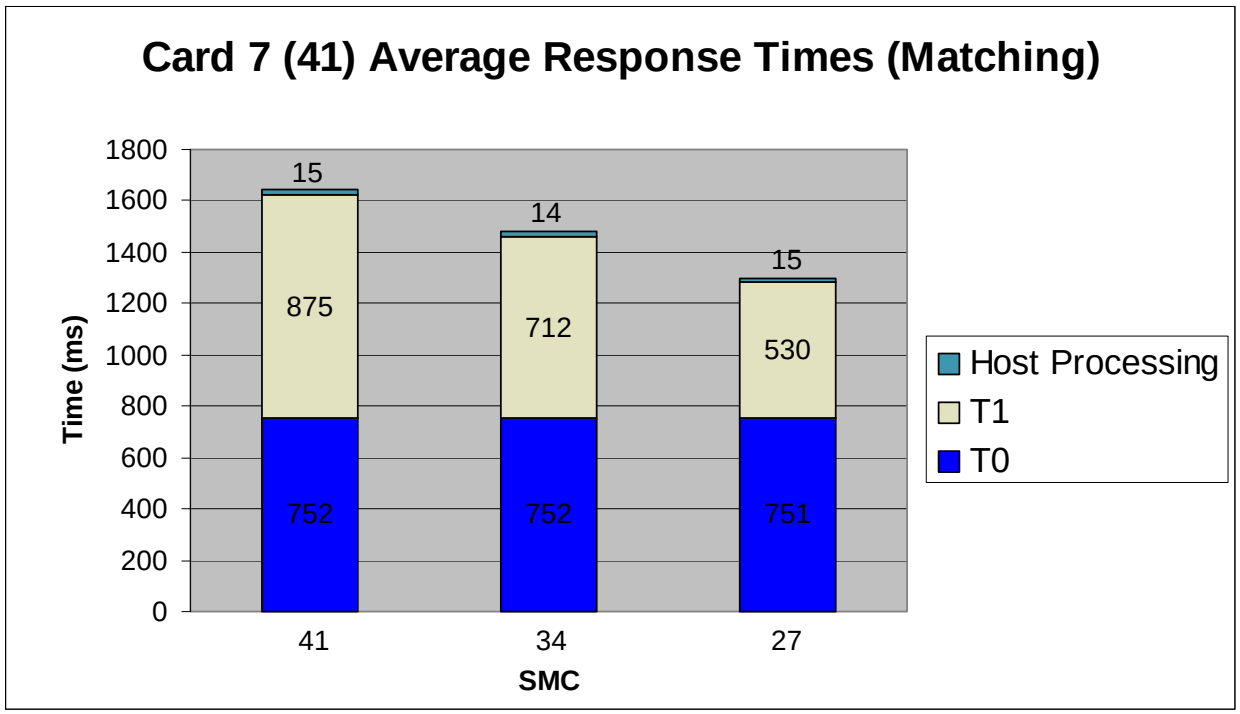


Figure B-29. Card 7 (41) Average Response Times for Matching Templates

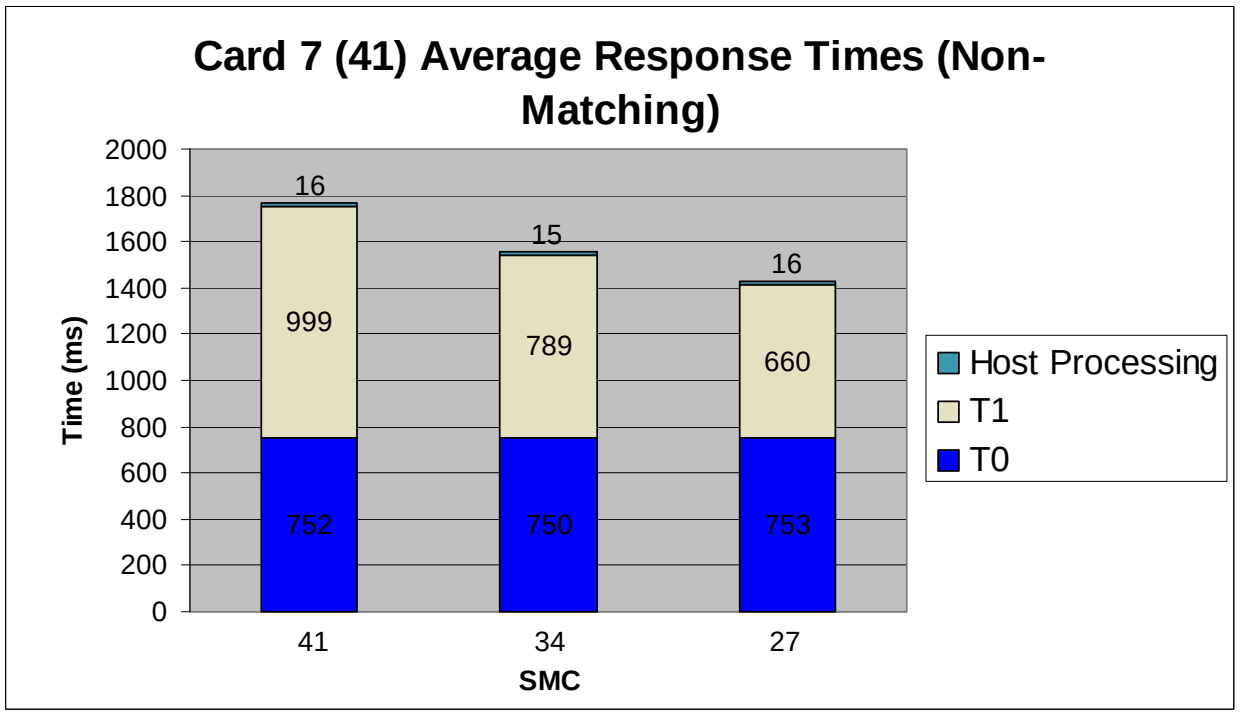


Figure B-30. Card 7 (41) Average Response Times for Non-Matching Templates

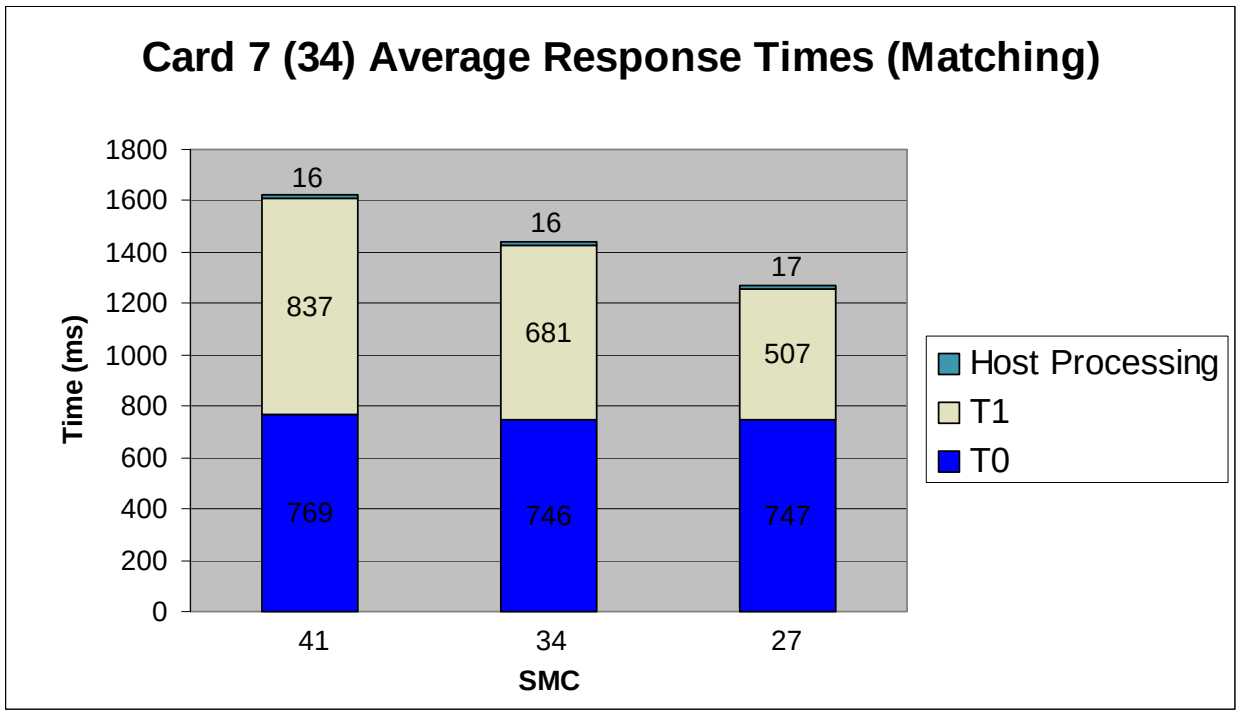


Figure B-31. Card 7 (34) Average Response Times for Matching Templates

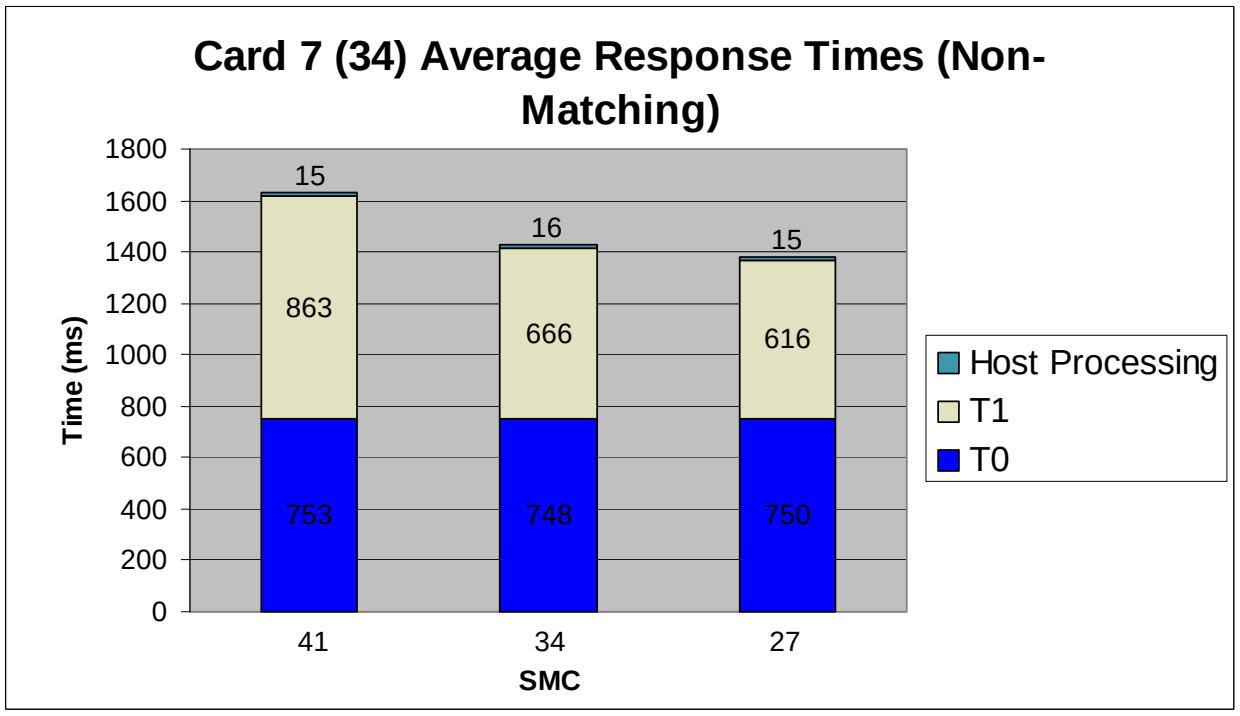


Figure B-32. Card 7 (34) Average Response Times for Non-Matching Templates

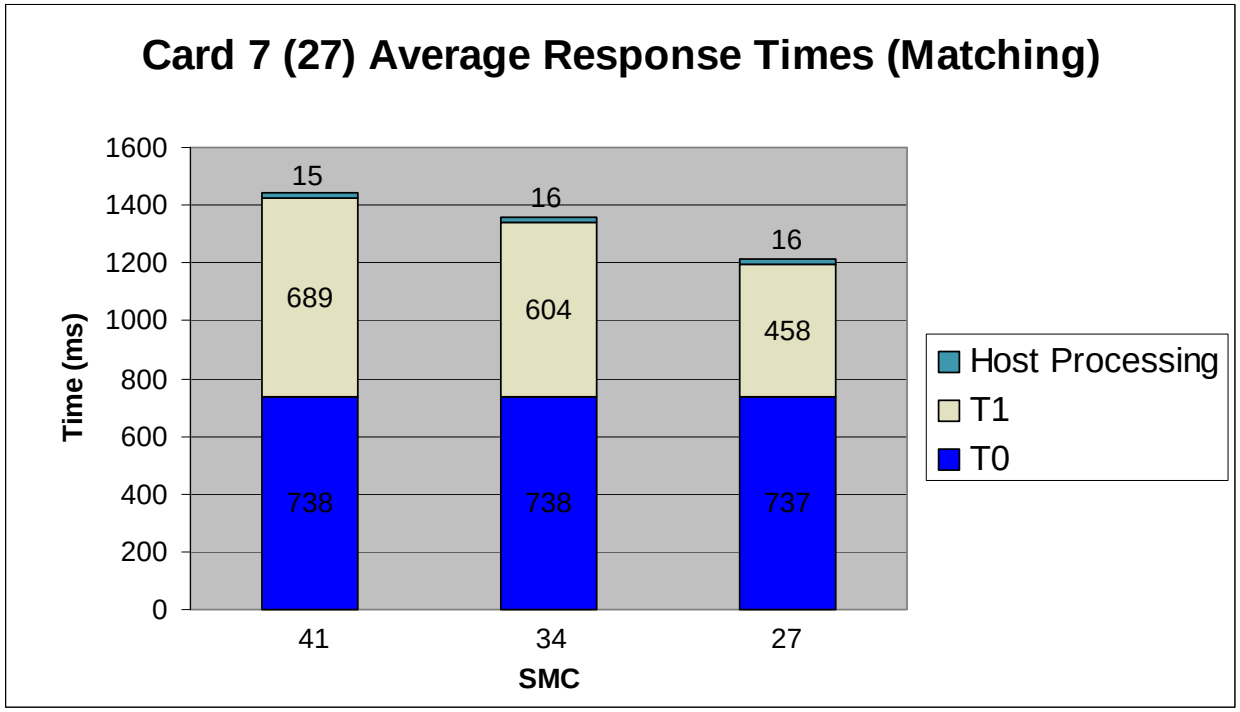


Figure B-33. Card 7 (27) Average Response Times for Matching Templates

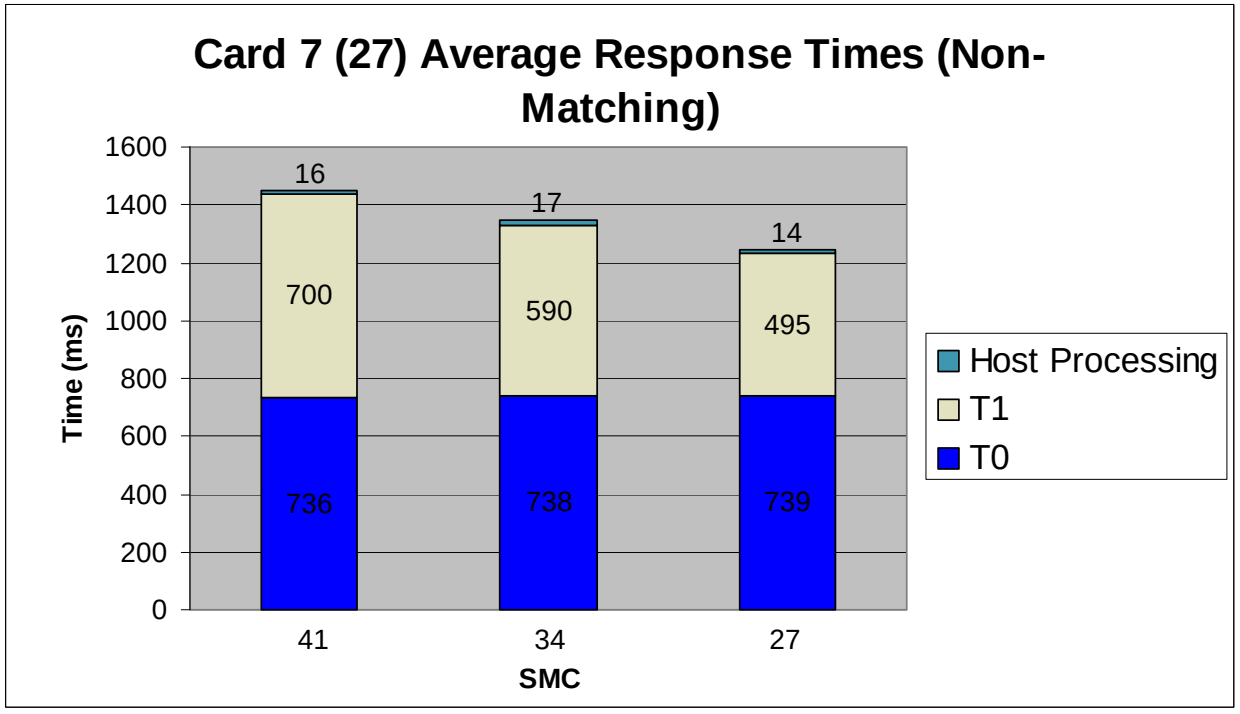


Figure B-34. Card 7 (27) Average Response Times for Non-Matching Templates

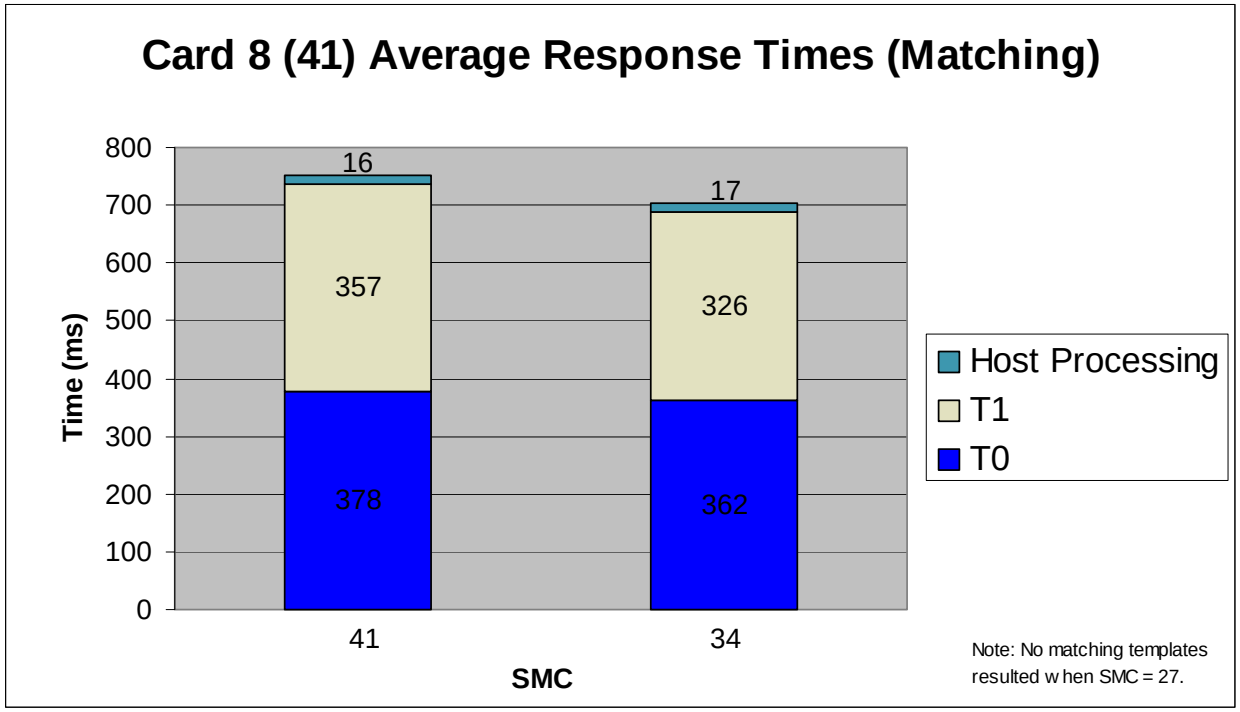


Figure B-35. Card 8 (41) Average Response Times for Matching Templates

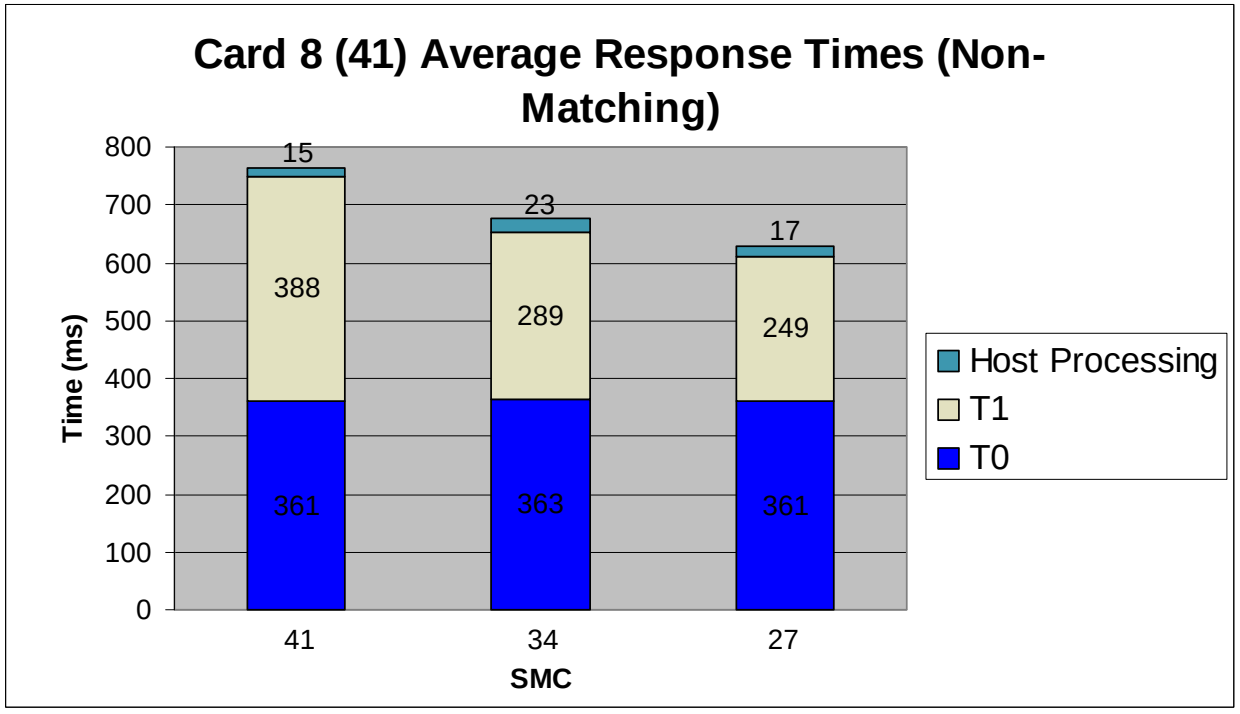


Figure B-36. Card 8 (41) Average Response Times for Non-Matching Templates

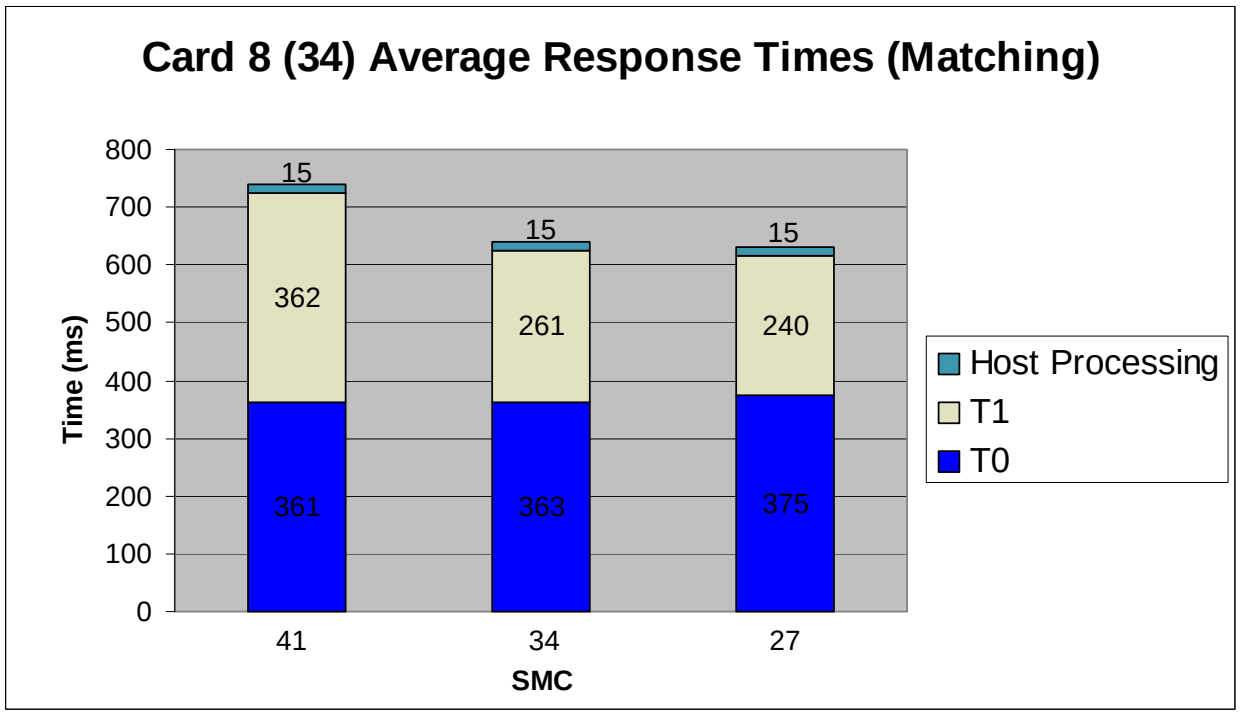


Figure B-37. Card 8 (34) Average Response Times for Matching Templates

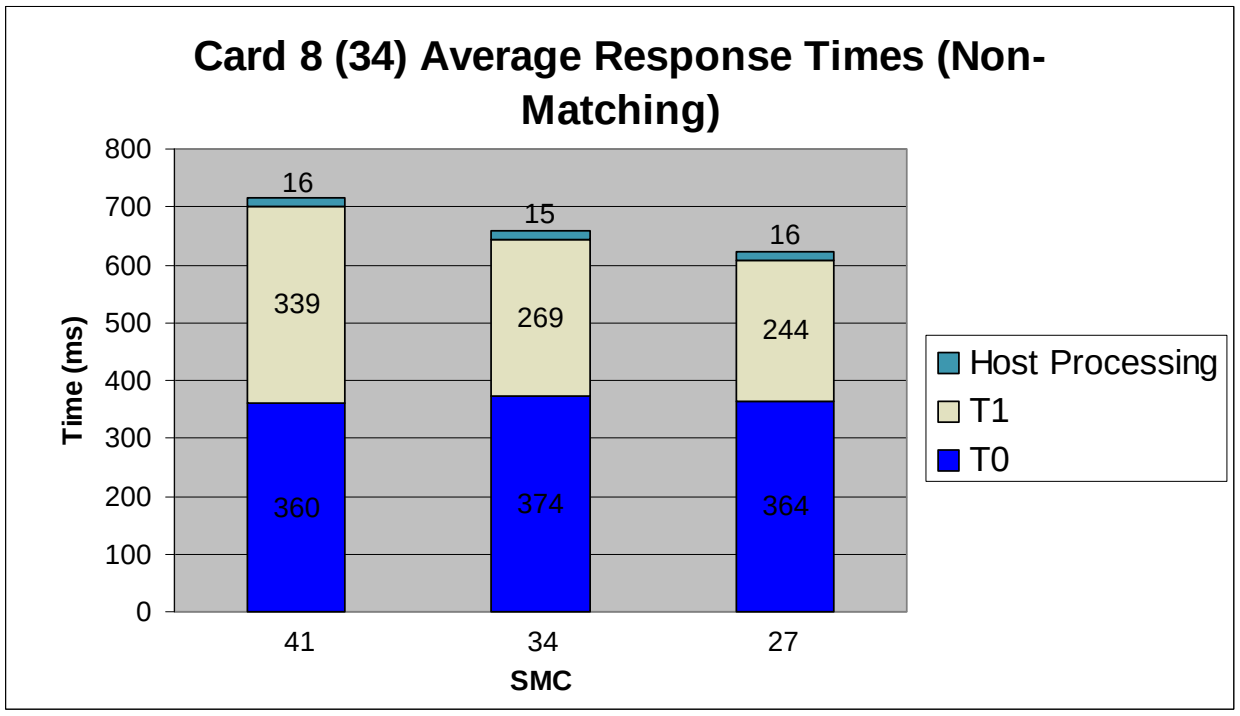


Figure B-38. Card 8 (34) Average Response Times for Non-Matching Templates

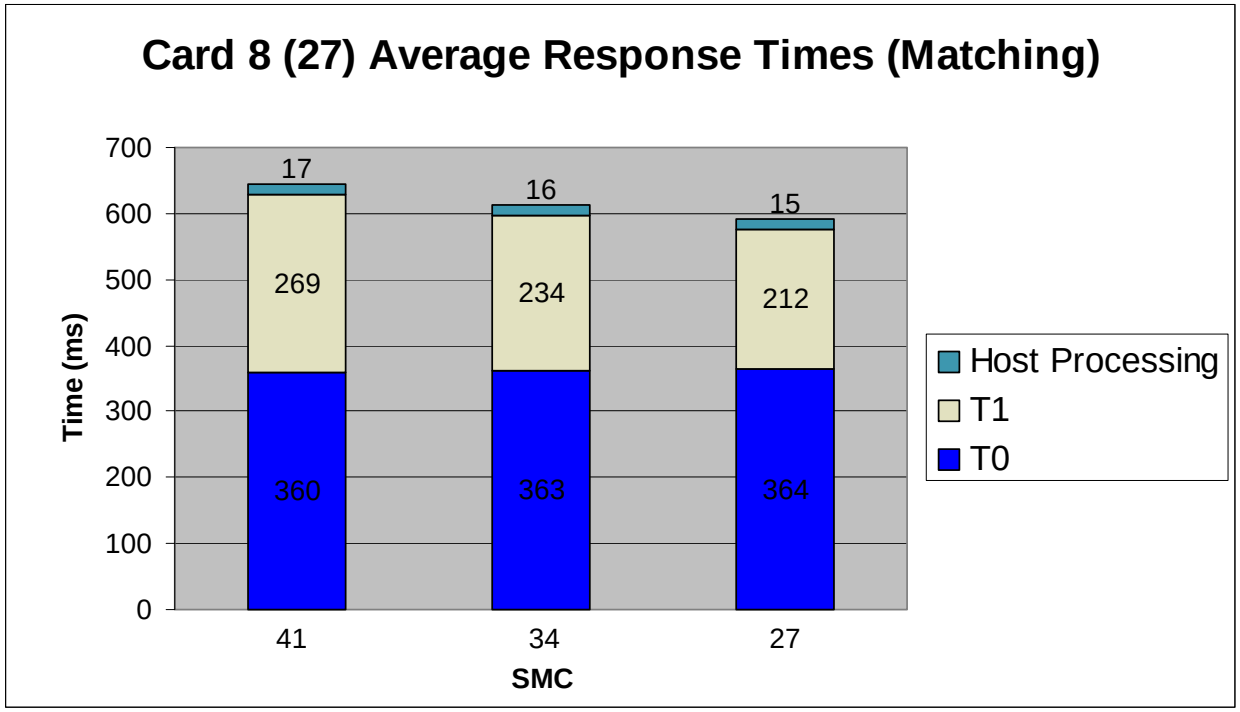


Figure B-39. Card 8 (27) Average Response Times for Matching Templates

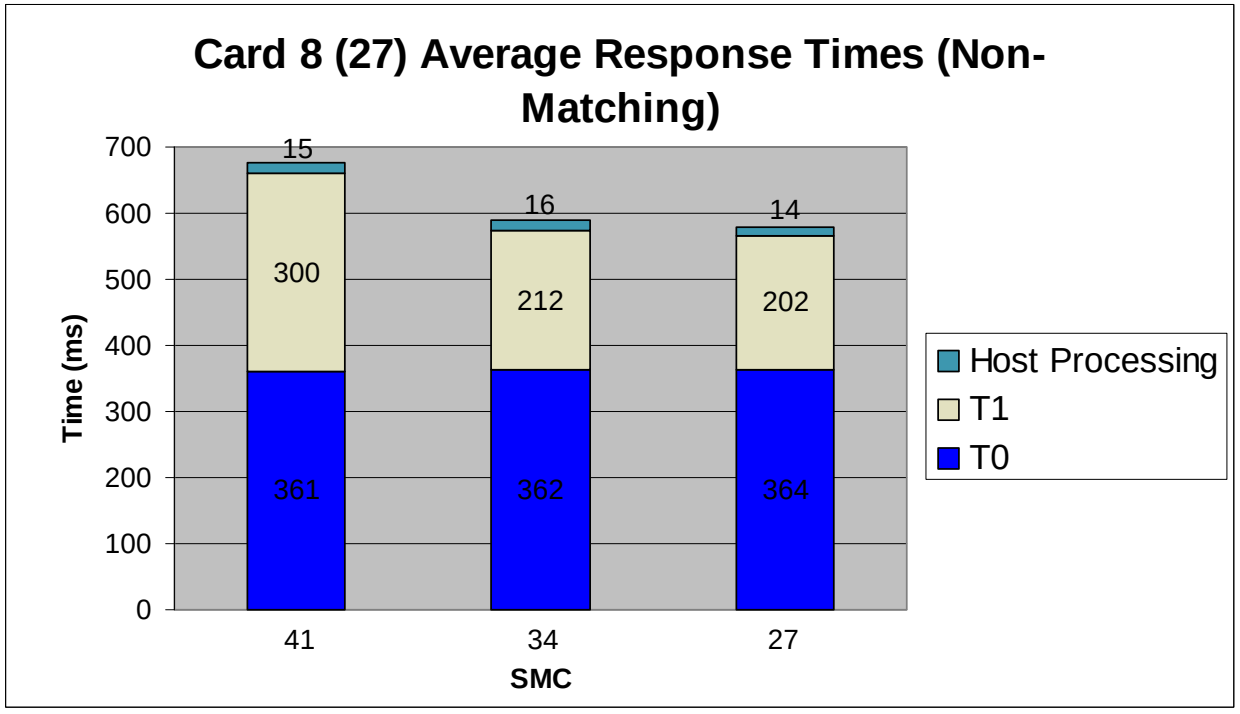


Figure B-40. Card 8 (27) Average Response Times for Non-Matching Templates

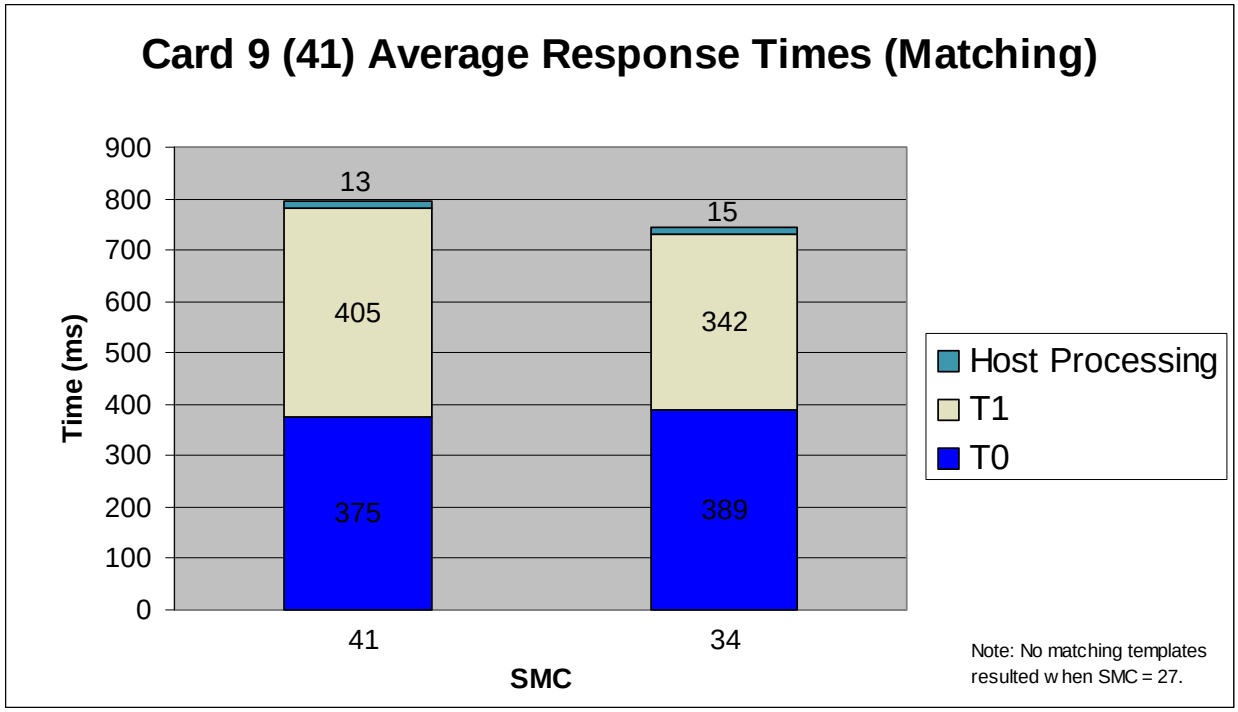


Figure B-41. Card 9 (41) Average Response Times for Matching Templates

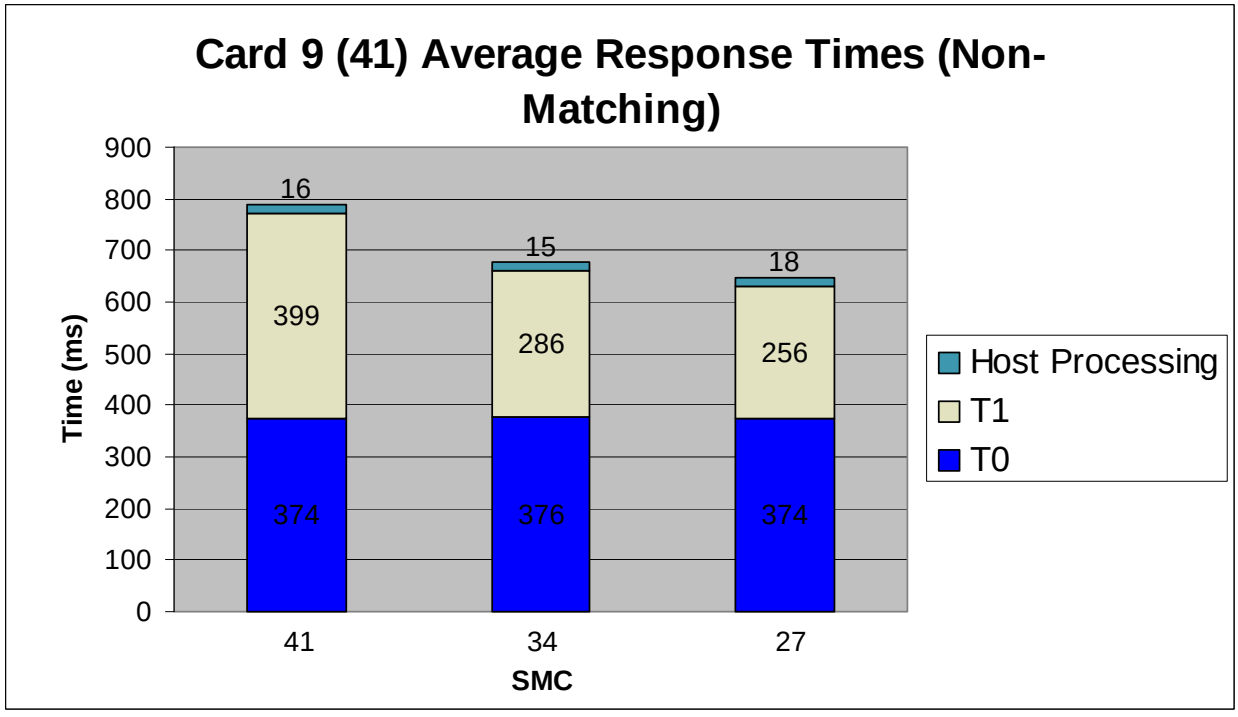


Figure B-42. Card 9 (41) Average Response Times for Non-Matching Templates

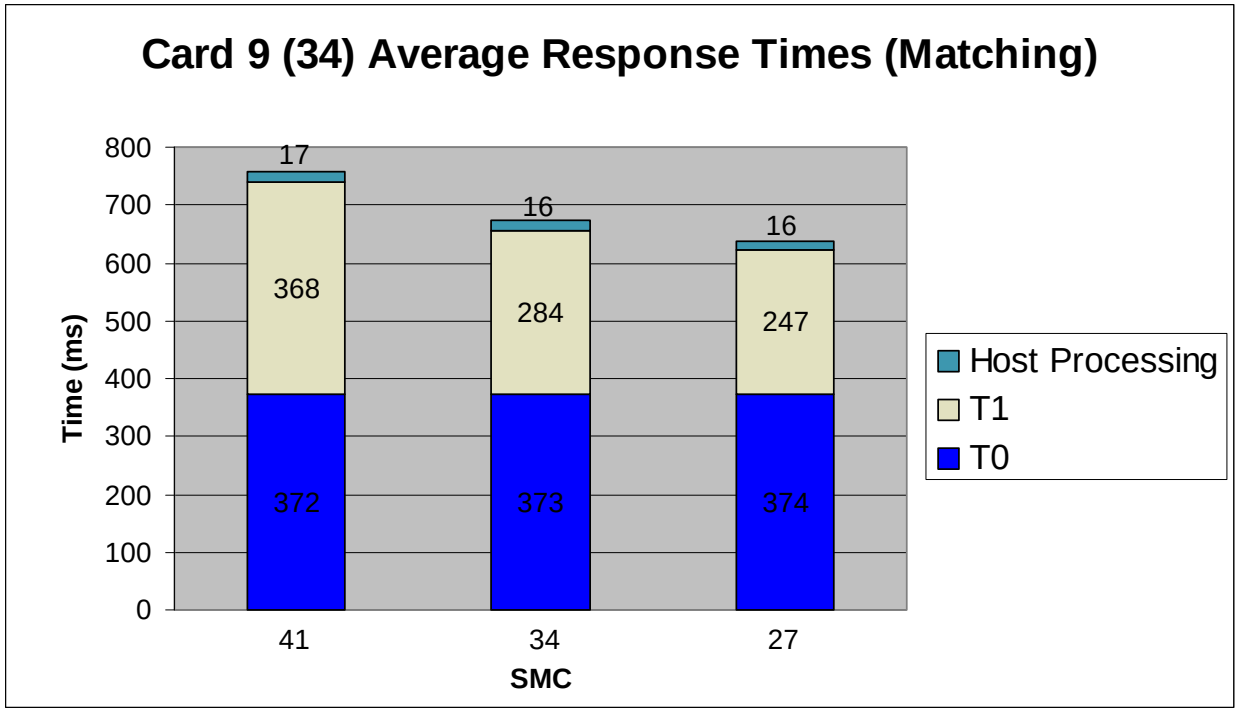


Figure B-43. Card 9 (34) Average Response Times for Matching Templates

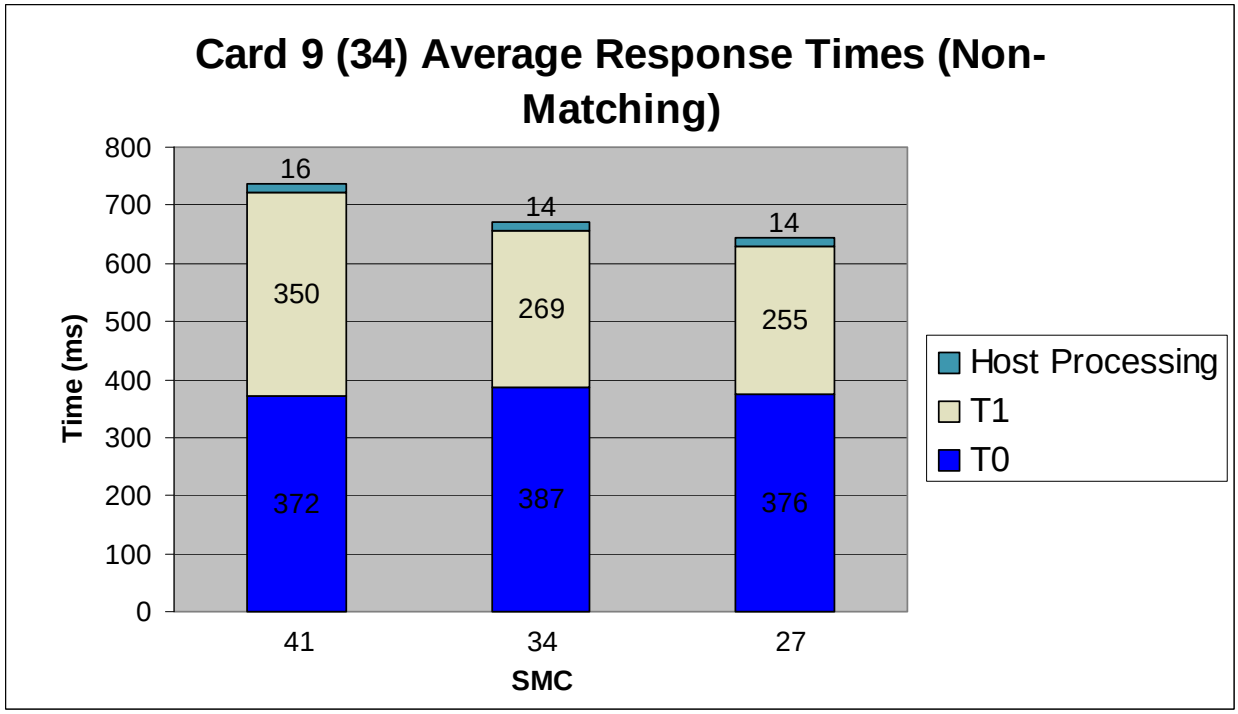


Figure B-44. Card 9 (34) Average Response Times for Non-Matching Templates

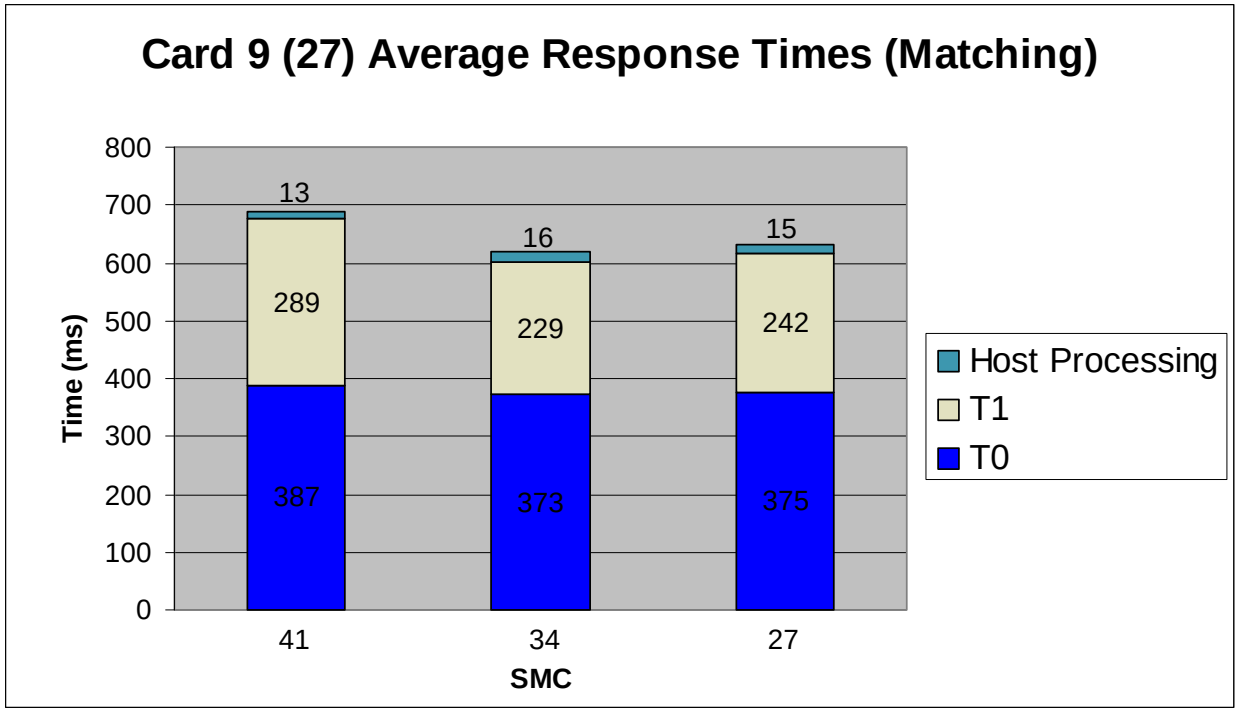


Figure B-45. Card 9 (27) Average Response Times for Matching Templates

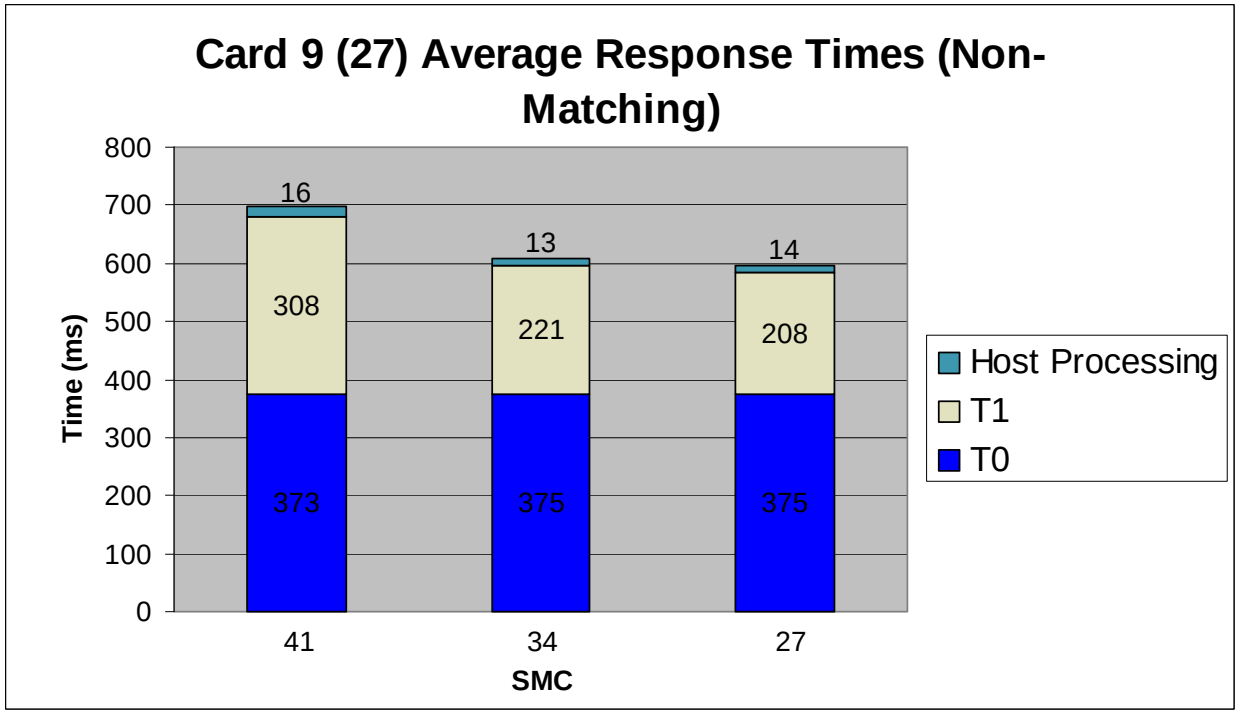


Figure B-46. Card 9 (27) Average Response Times for Non-Matching Templates

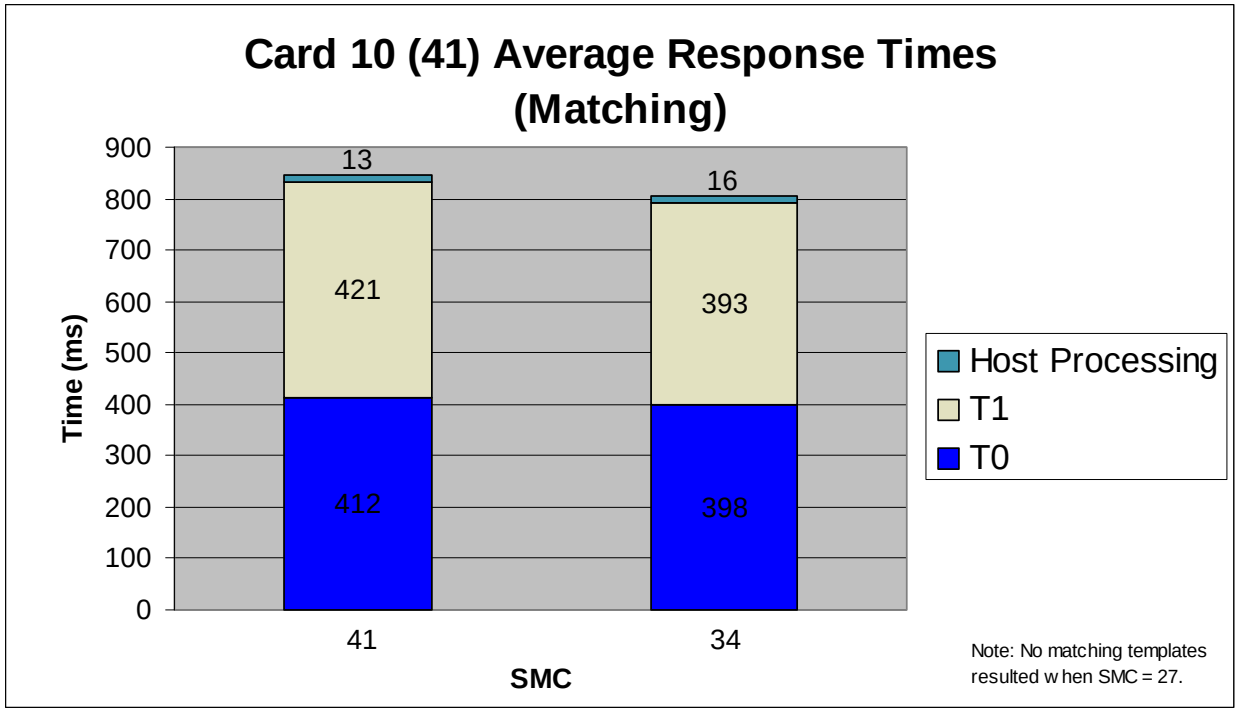


Figure B-47. Card 10 (41) Average Response Times for Matching Templates

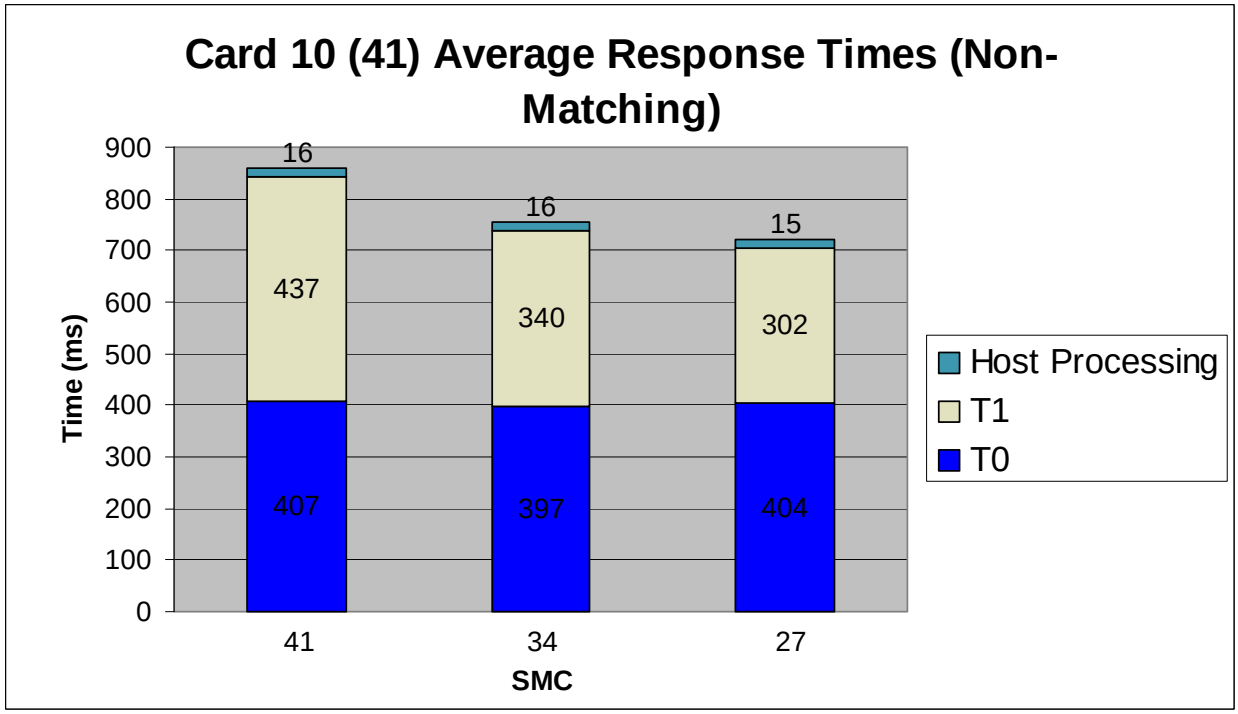


Figure B-48. Card 10 (41) Average Response Times for Non-Matching Templates

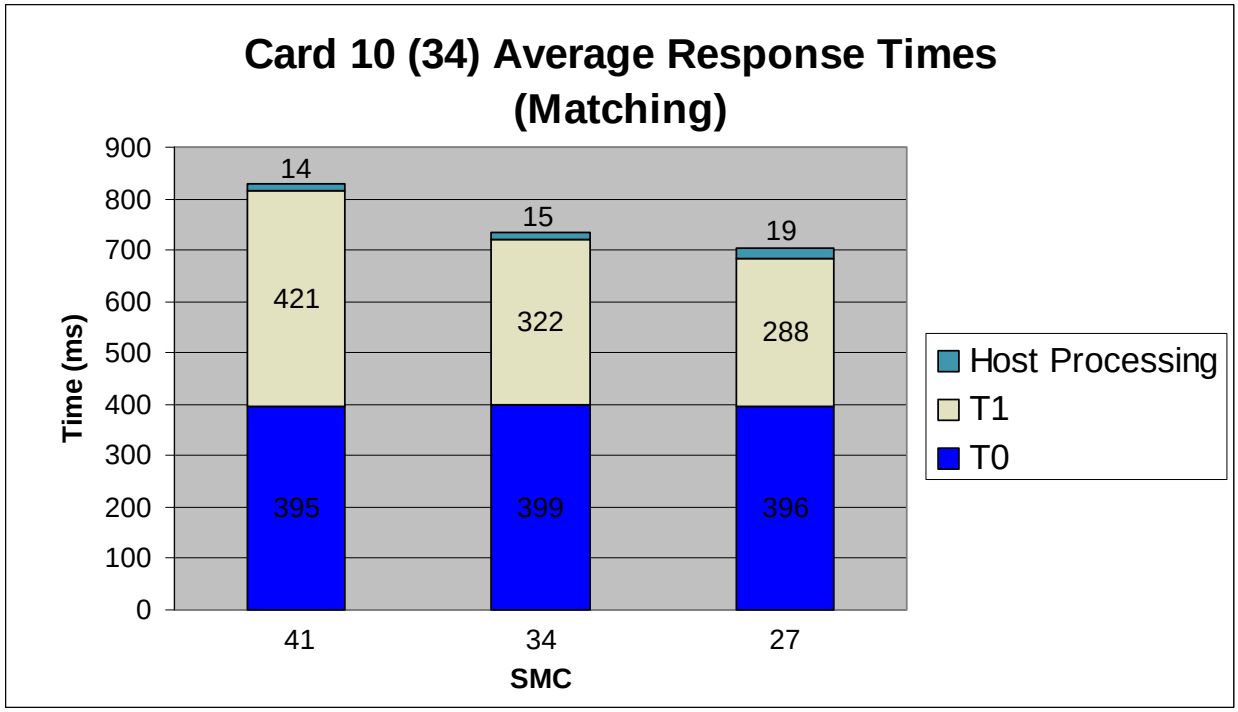


Figure B-49. Card 10 (34) Average Response Times for Matching Templates

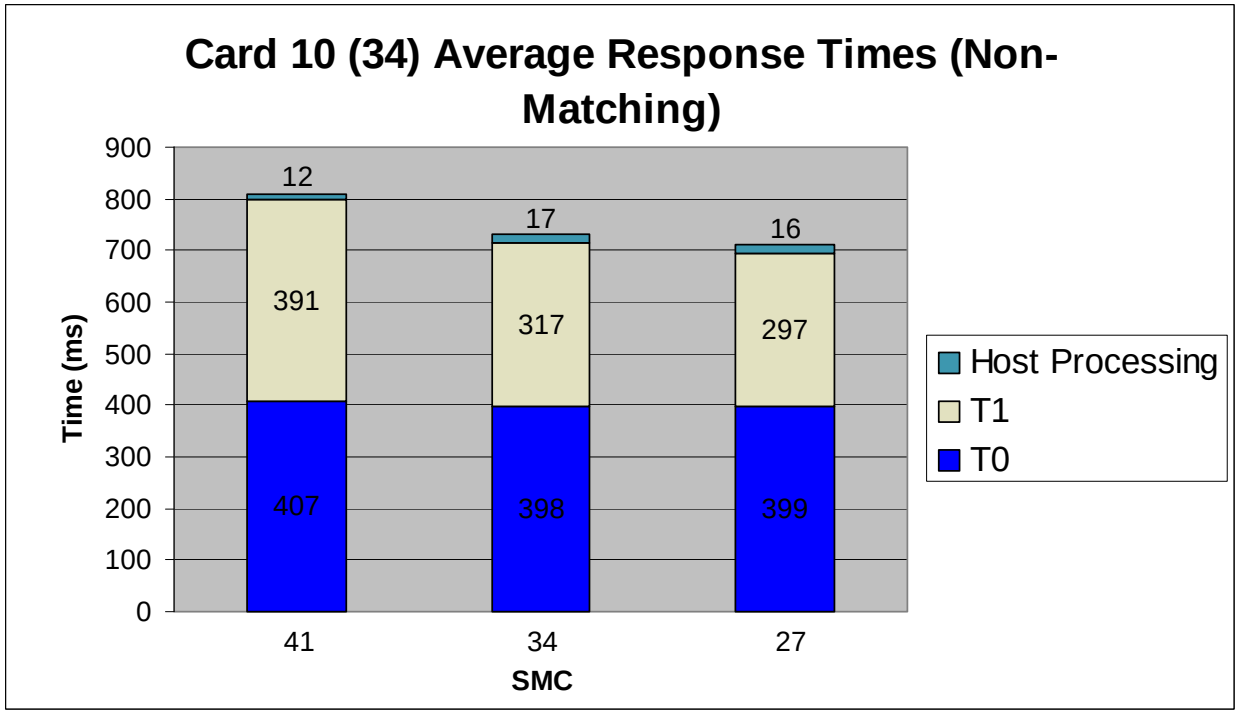


Figure B-50. Card 10 (34) Average Response Times for Non-Matching Templates

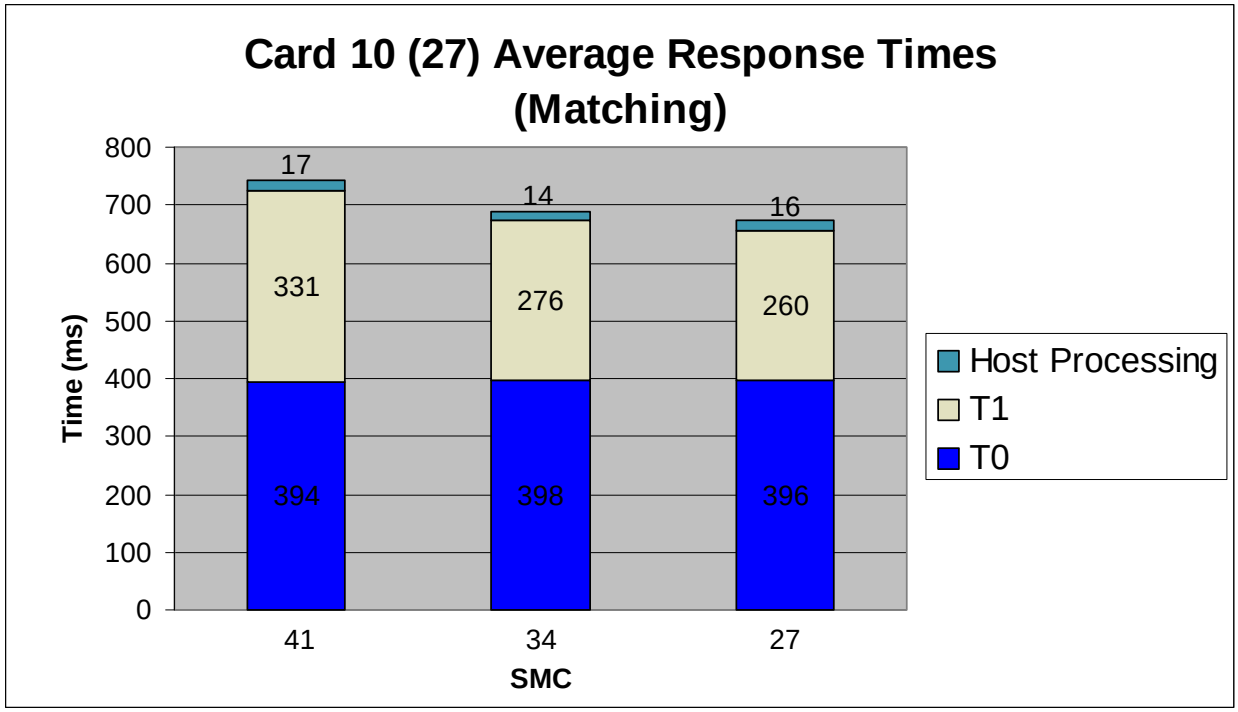


Figure B-51. Card 10 (27) Average Response Times for Matching Templates

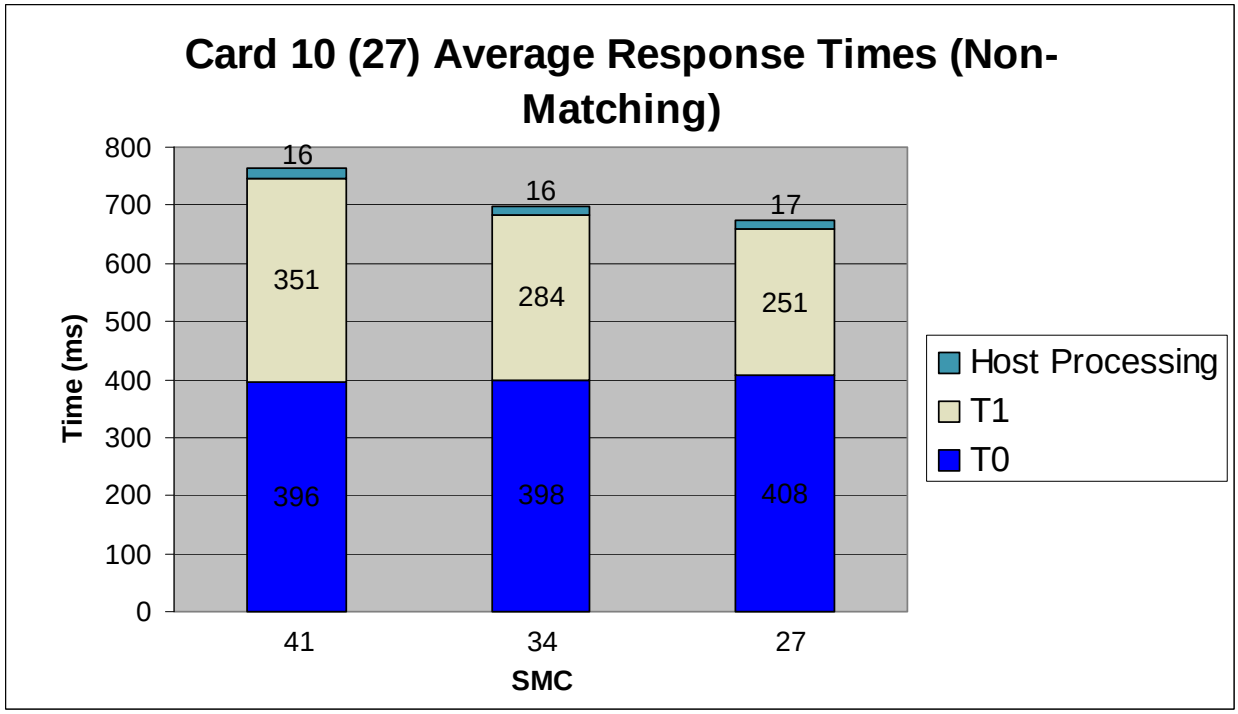


Figure B-52. Card 10 (27) Average Response Times for Non-Matching Templates

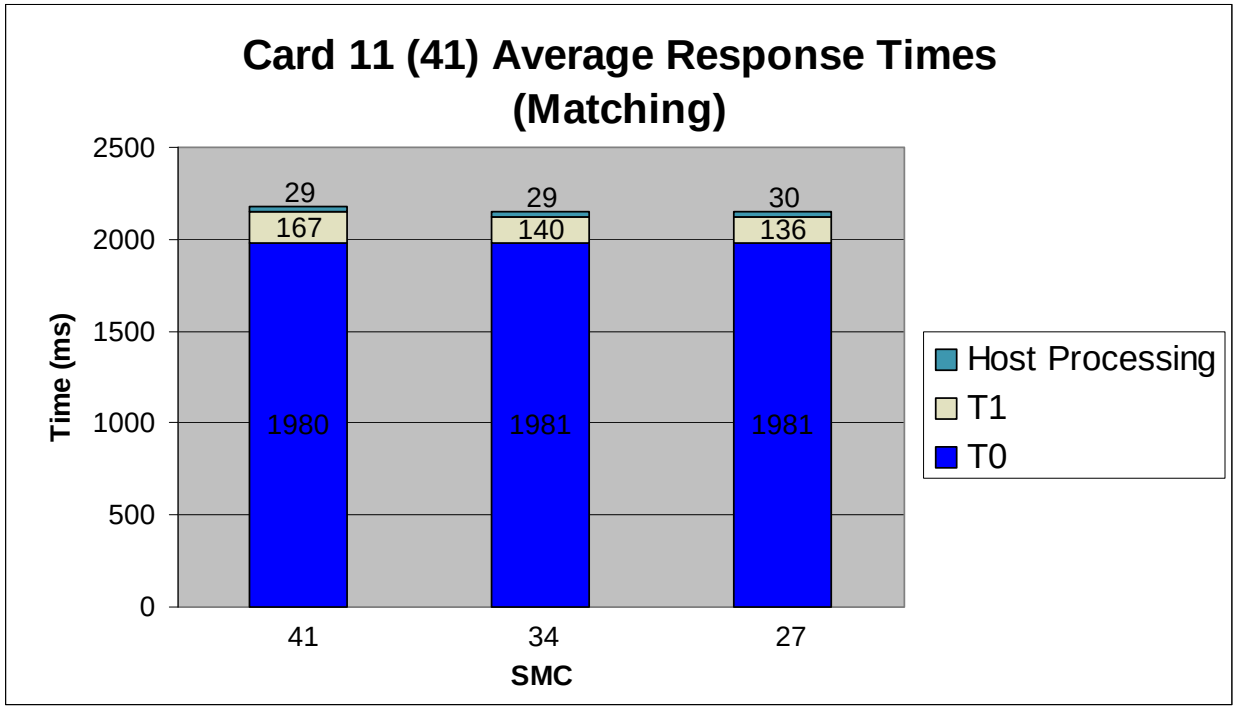


Figure B-53. Card 11 (41) Average Response Times for Matching Templates

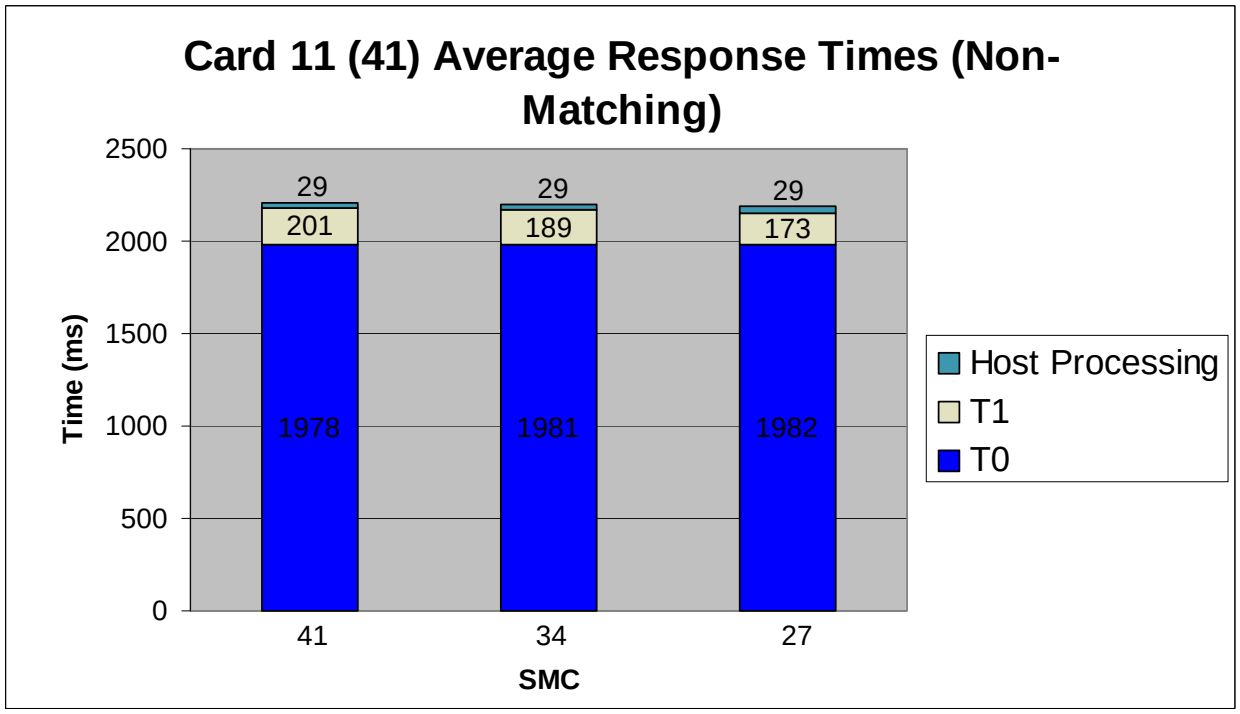


Figure B-54. Card 11 (41) Average Response Times for Non-Matching Templates

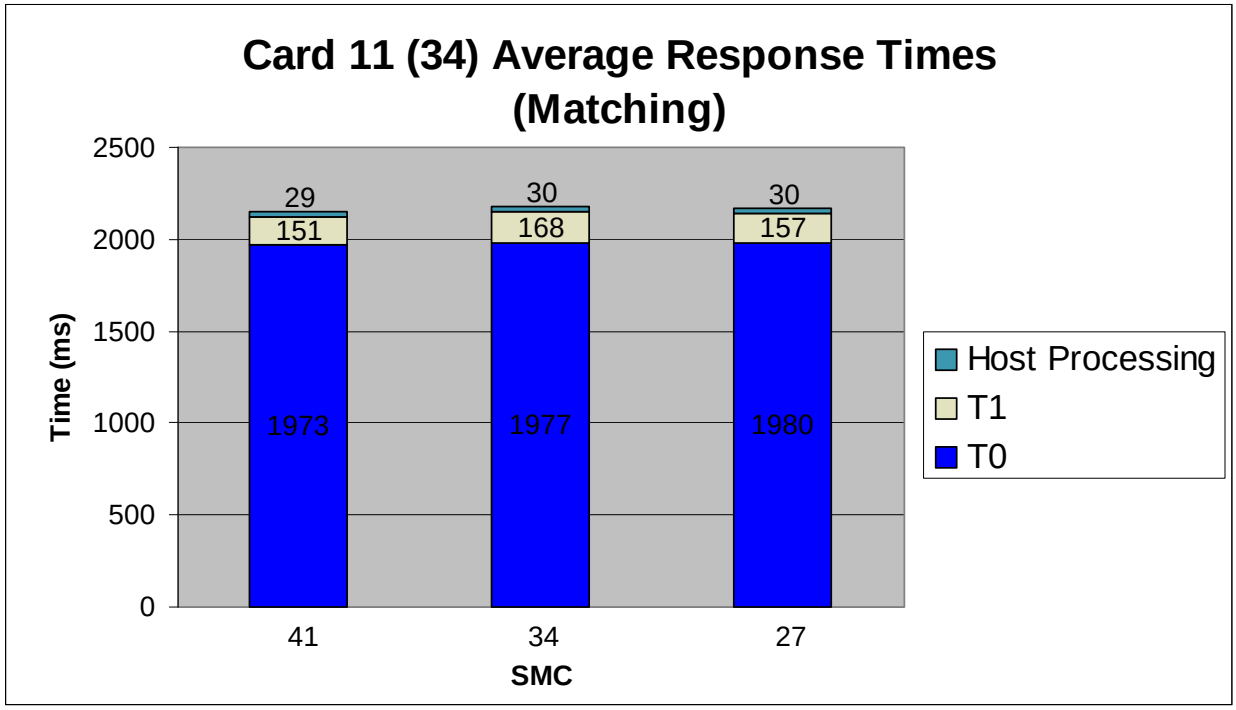


Figure B-55. Card 11 (34) Average Response Times for Matching Templates

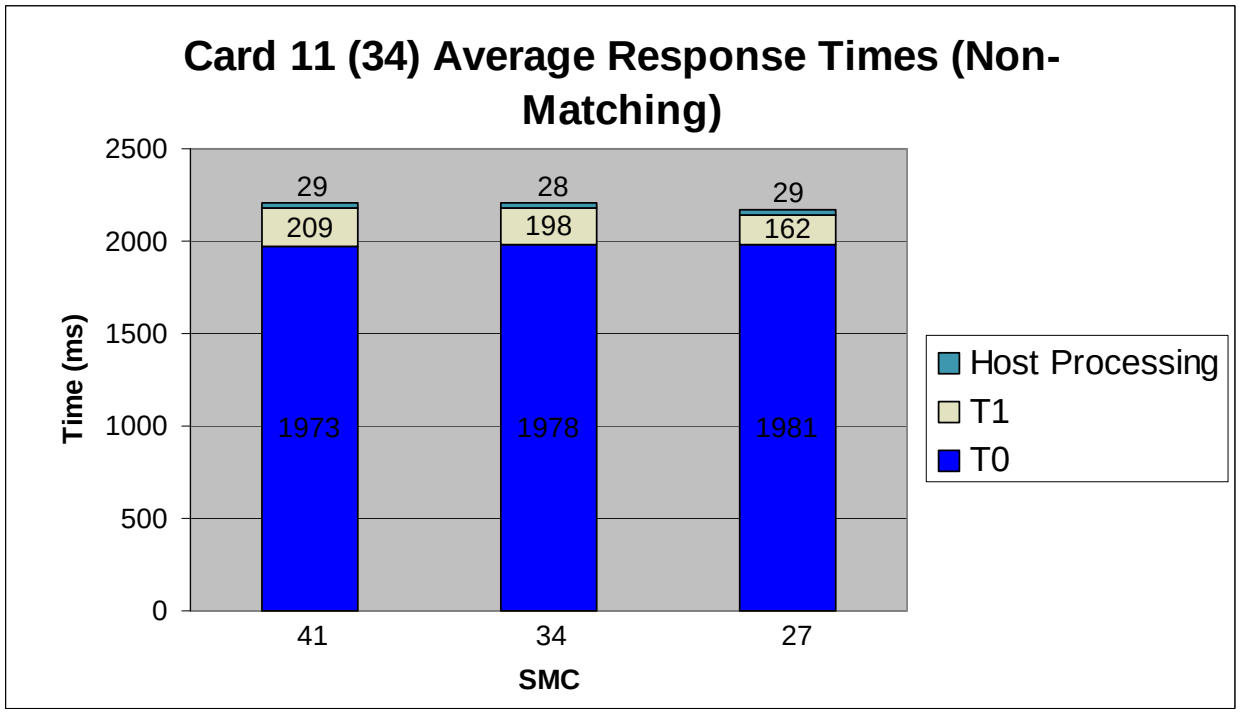


Figure B-56. Card 11 (34) Average Response Times for Non-Matching Templates

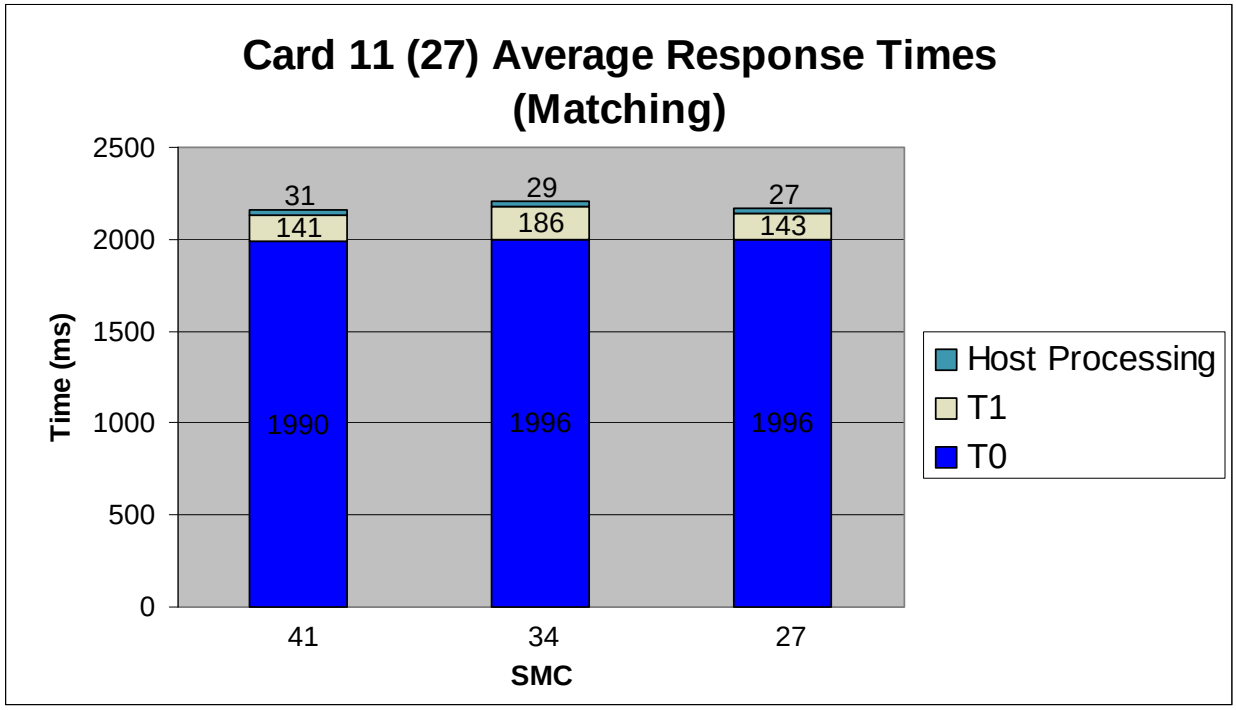


Figure B-57. Card 11 (27) Average Response Times for Matching Templates

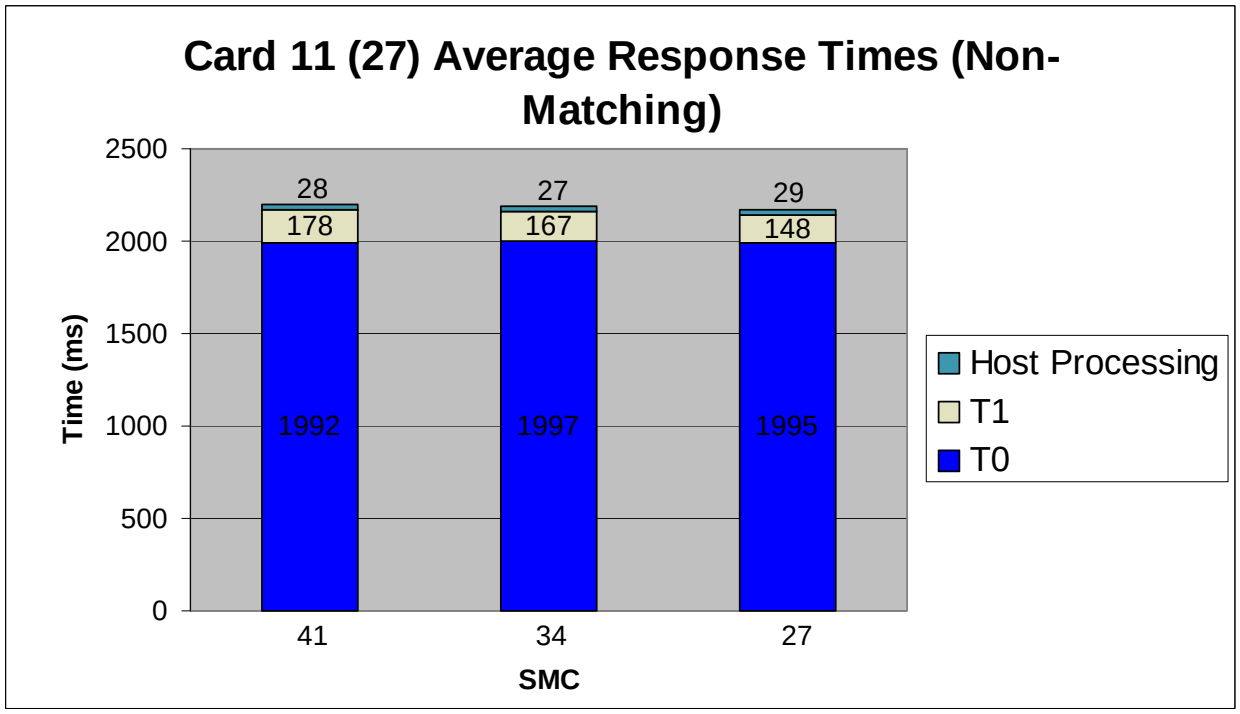


Figure B-58. Card 11 (27) Average Response Times for Non-Matching Templates

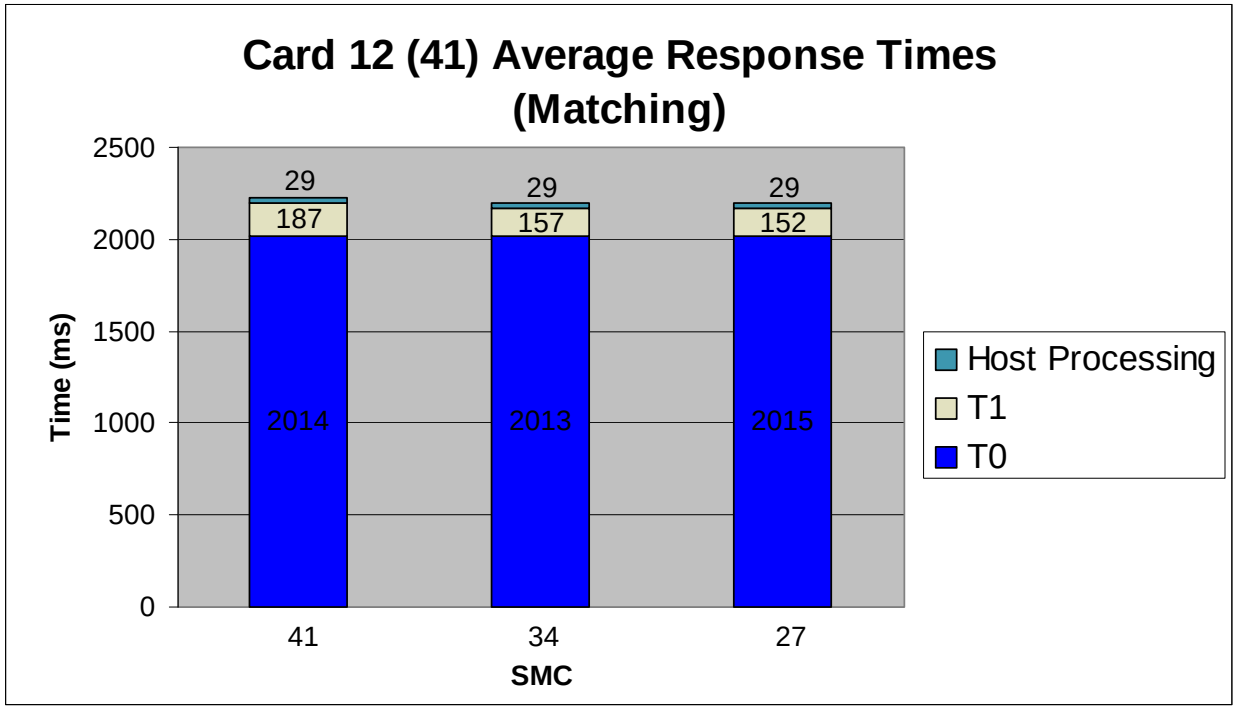


Figure B-59. Card 12 (41) Average Response Times for Matching Templates

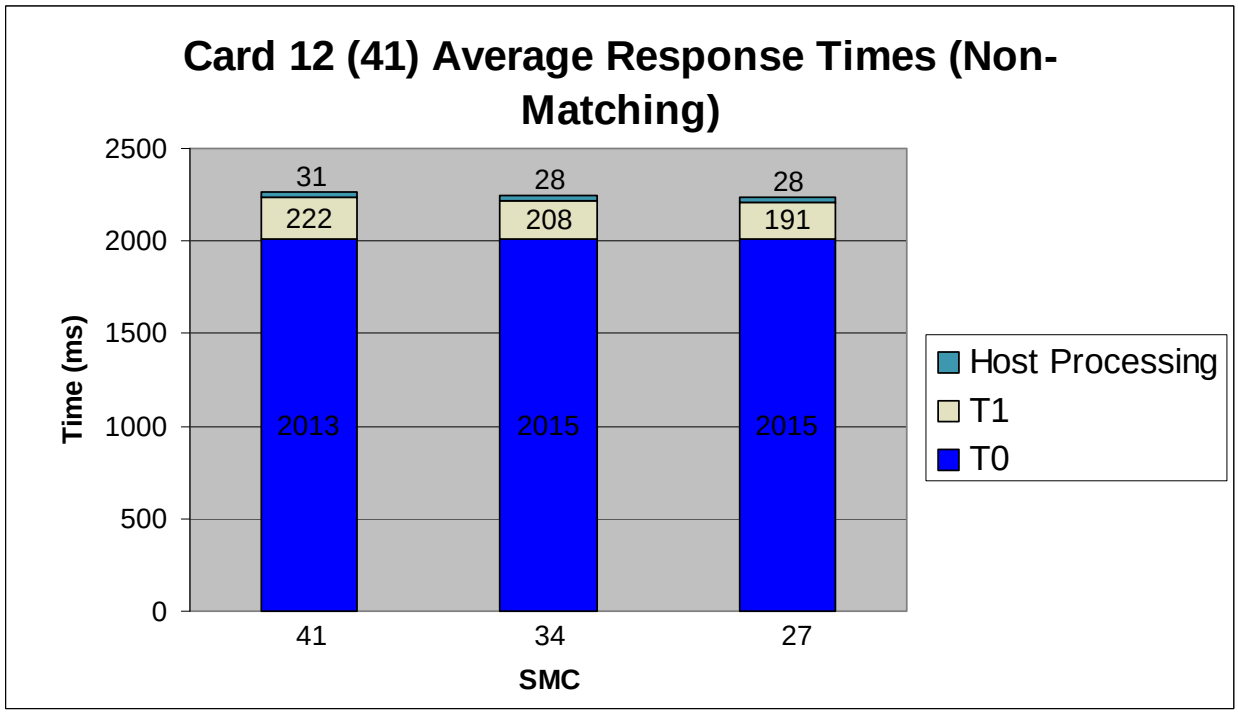


Figure B-60. Card 12 (41) Average Response Times for Non-Matching Templates

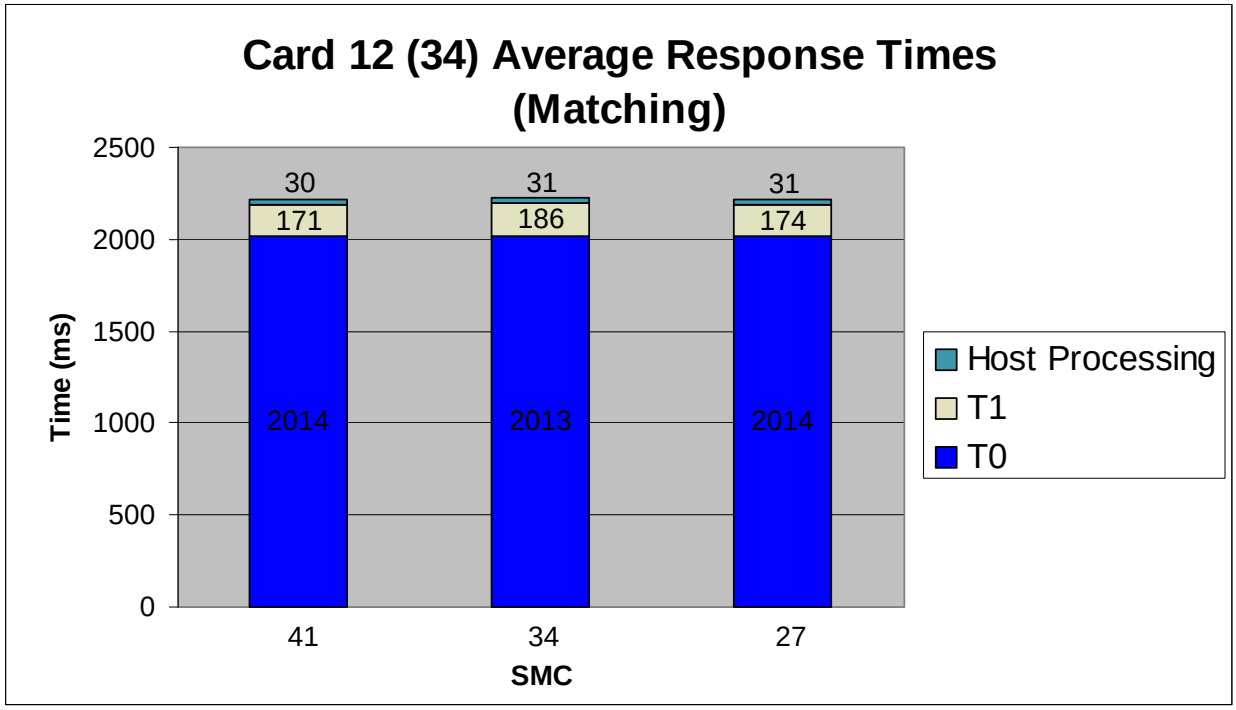


Figure B-61. Card 12 (34) Average Response Times for Matching Templates

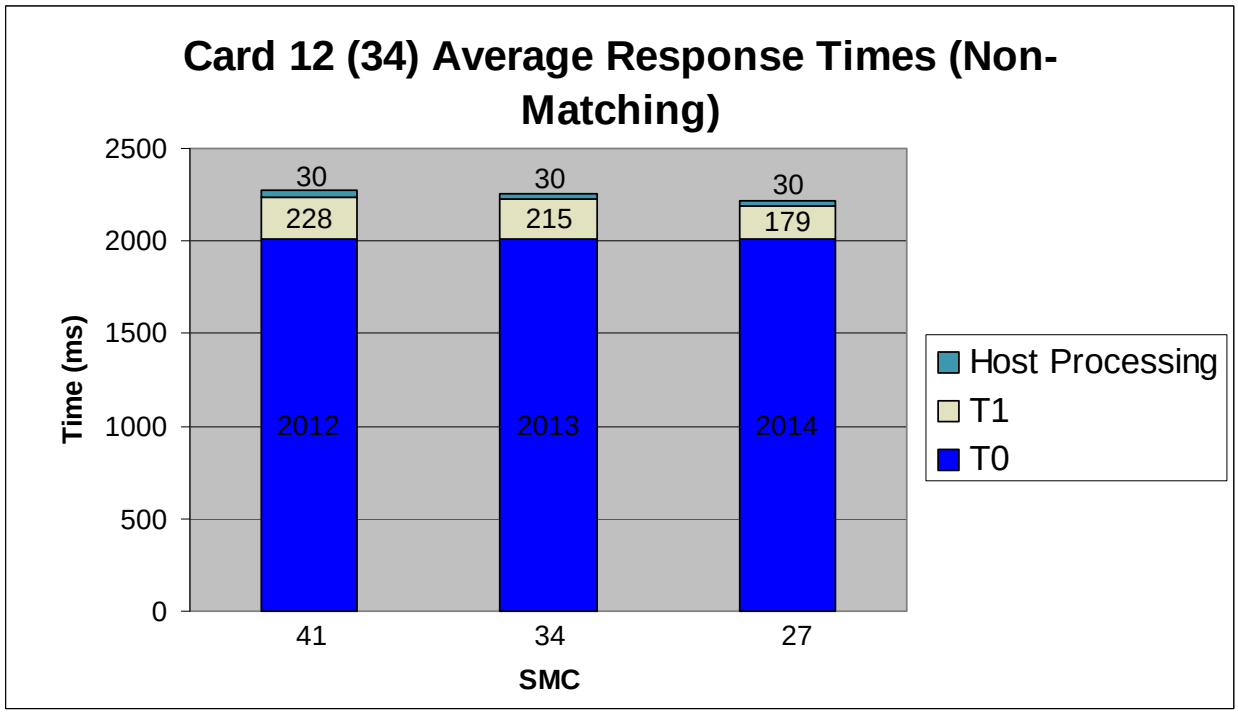


Figure B-62. Card 12 (34) Average Response Times for Non-Matching Templates

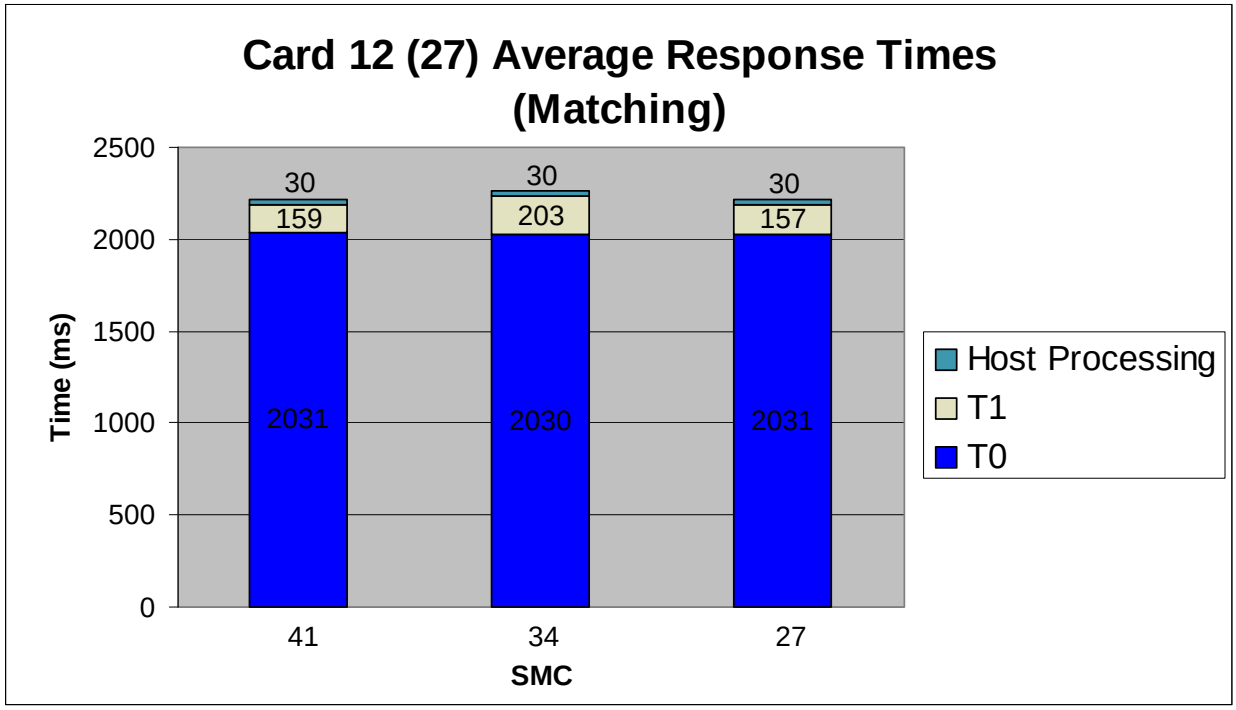


Figure B-63. Card 12 (27) Average Response Times for Matching Templates

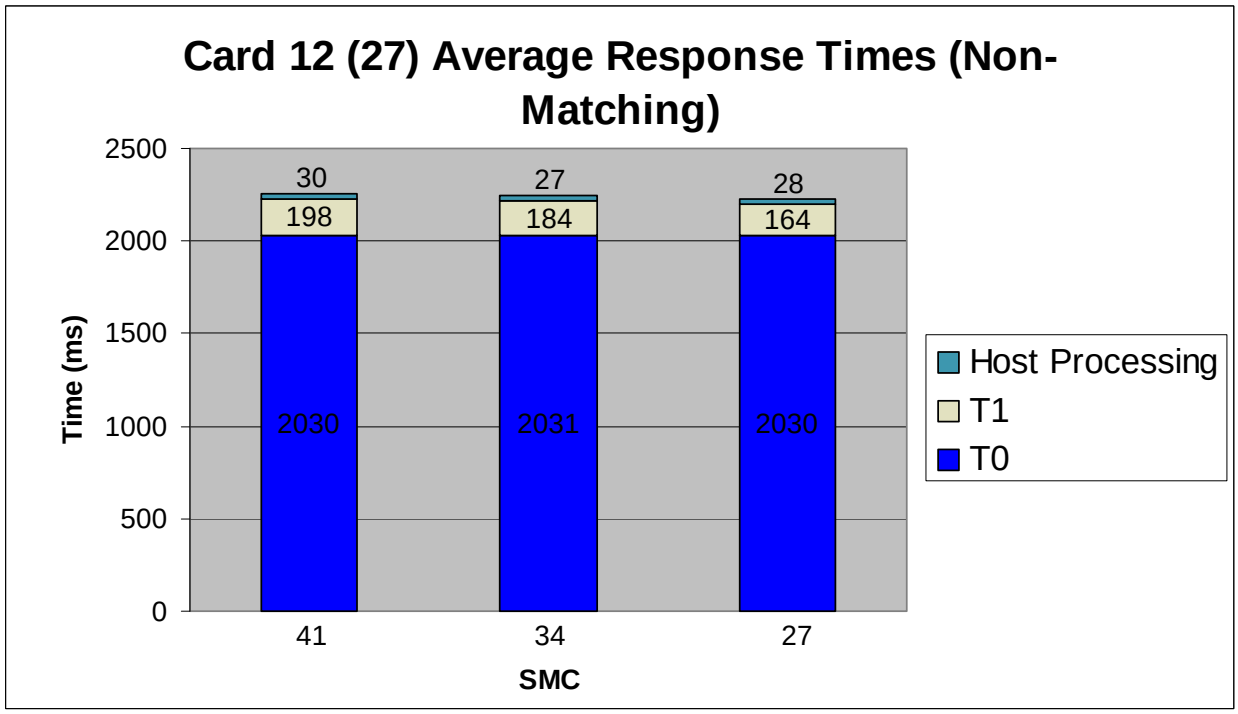


Figure B-64. Card 12 (27) Average Response Times for Non-Matching Templates

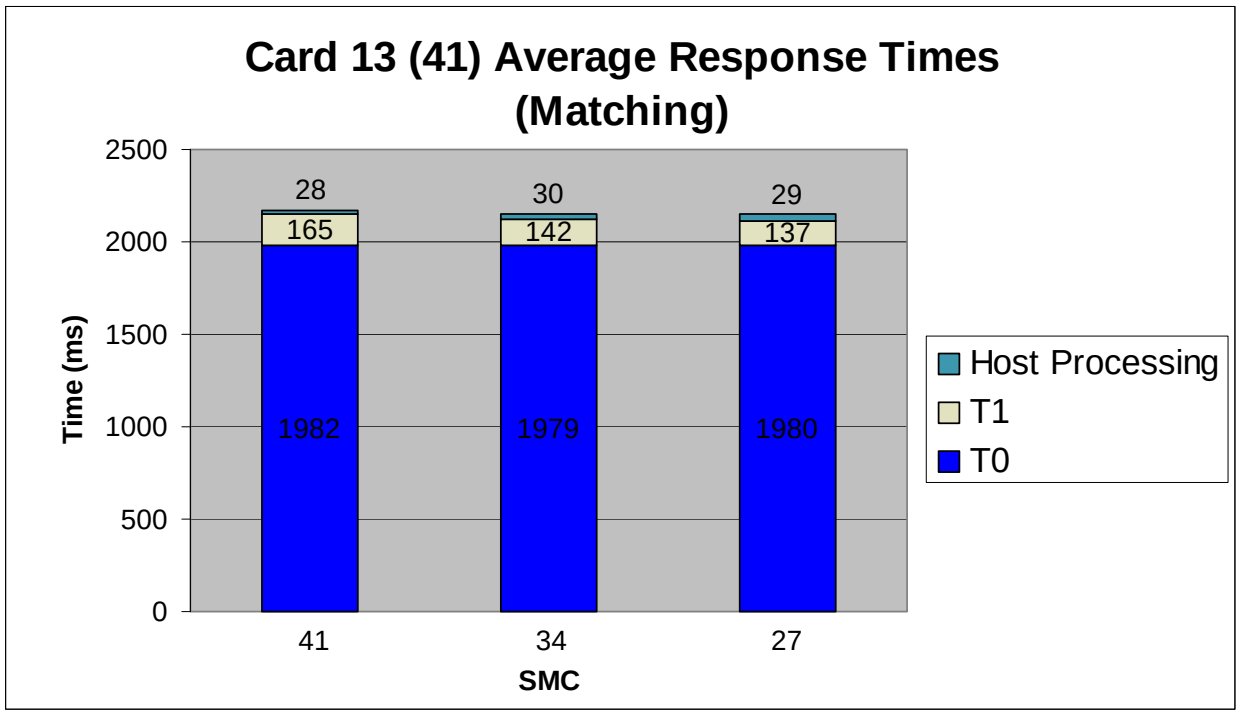


Figure B-65. Card 13 (41) Average Response Times for Matching Templates[5]

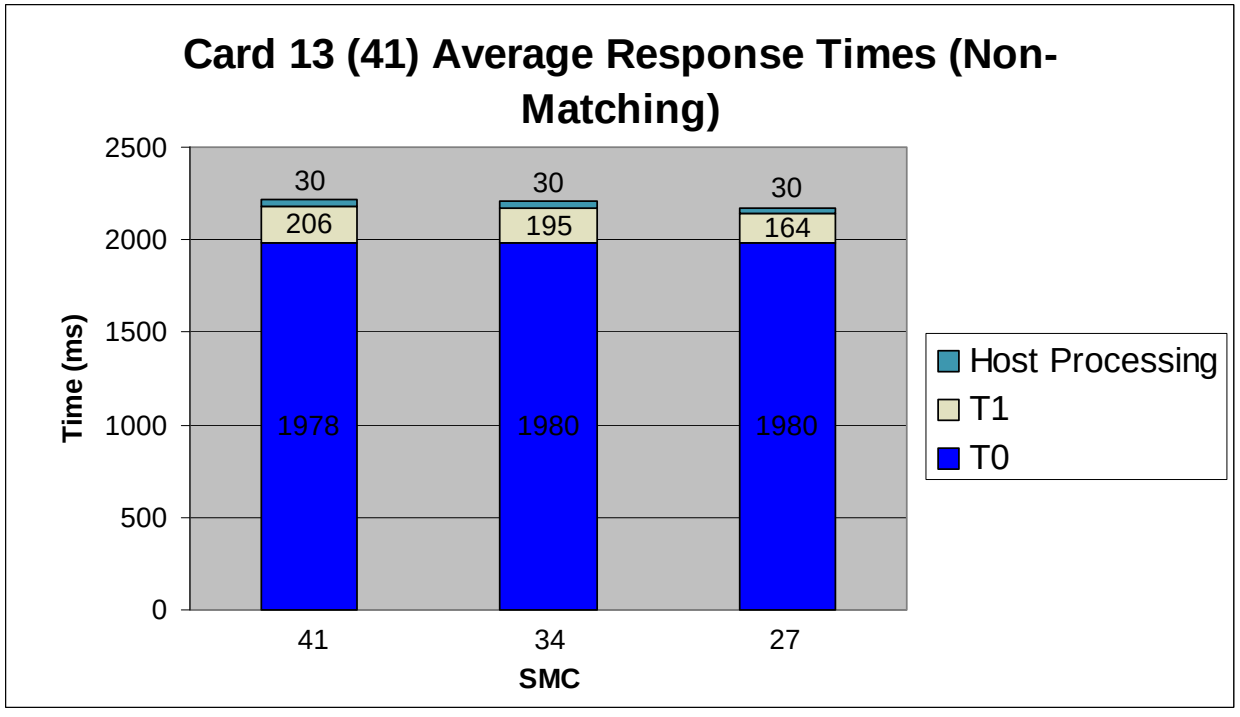


Figure B-66. Card 13 (41) Average Response Times for Non-Matching Templates

[5] Card 13 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

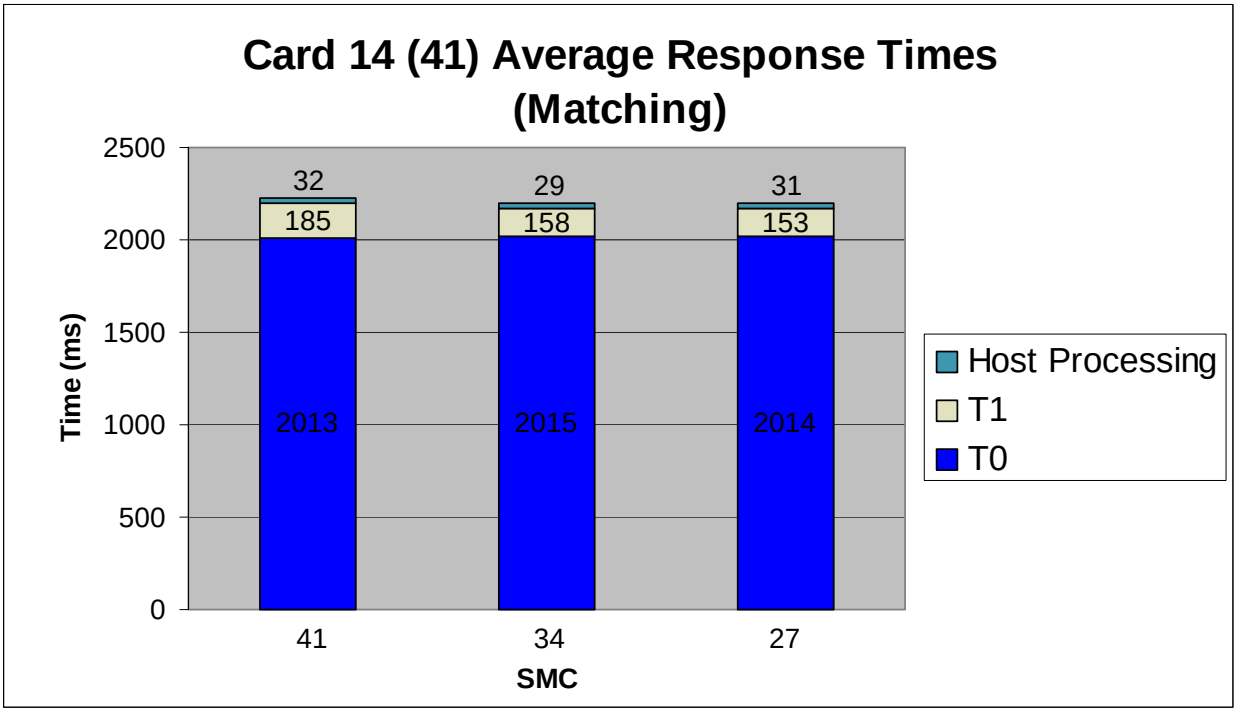


Figure B-67. Card 14 (41) Average Response Times for Matching Templates[6]

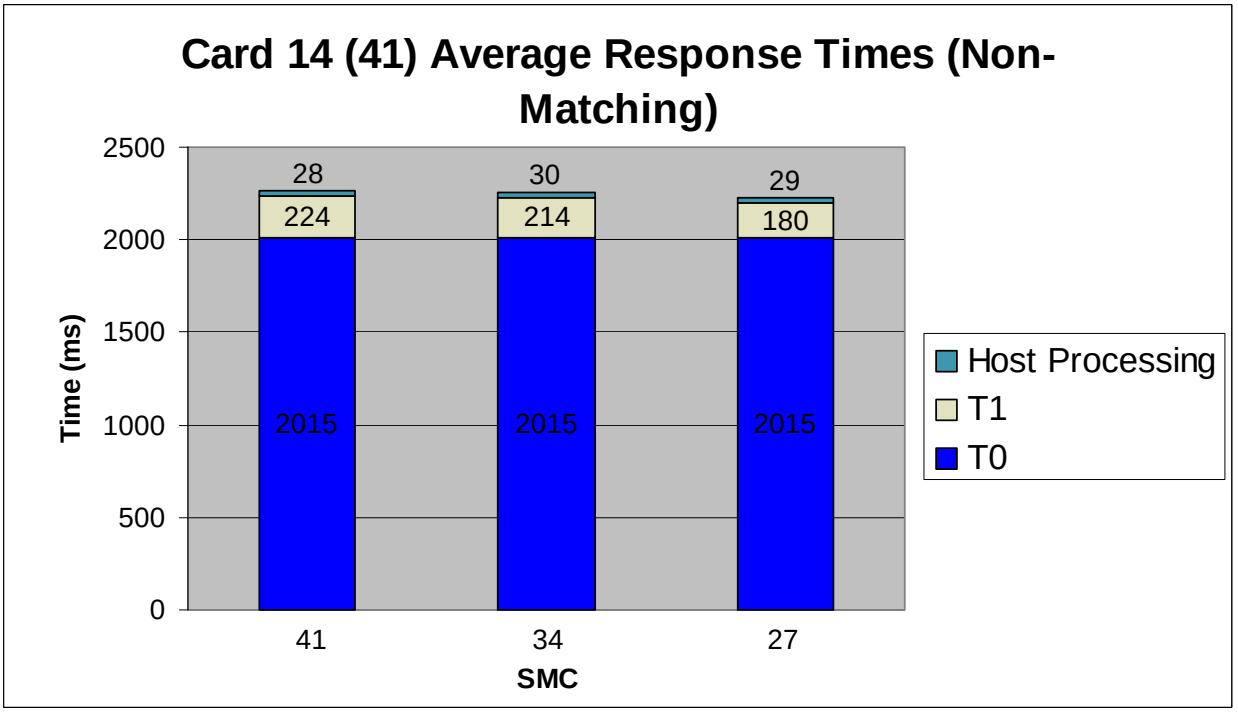


Figure B-68. Card 14 (41) Average Response Times for Non-Matching Templates

[6] Card 14 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

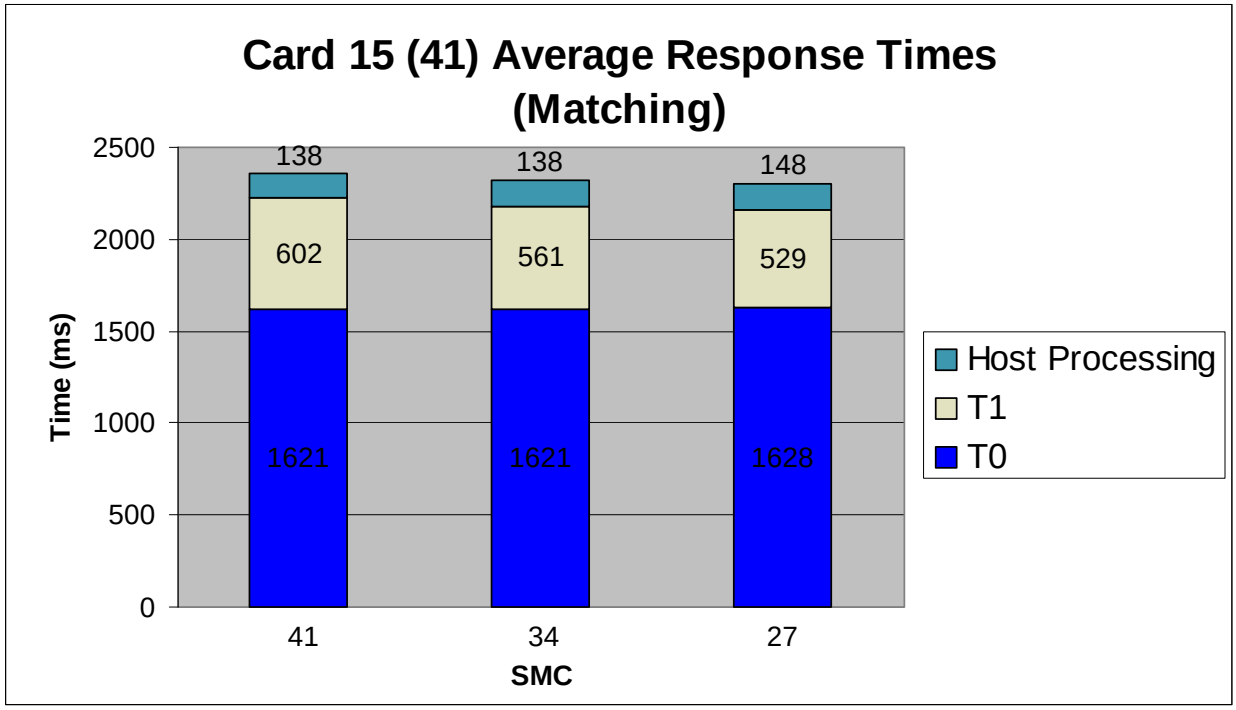


Figure B-69. Card 15 (41) Average Response Times for Matching Templates

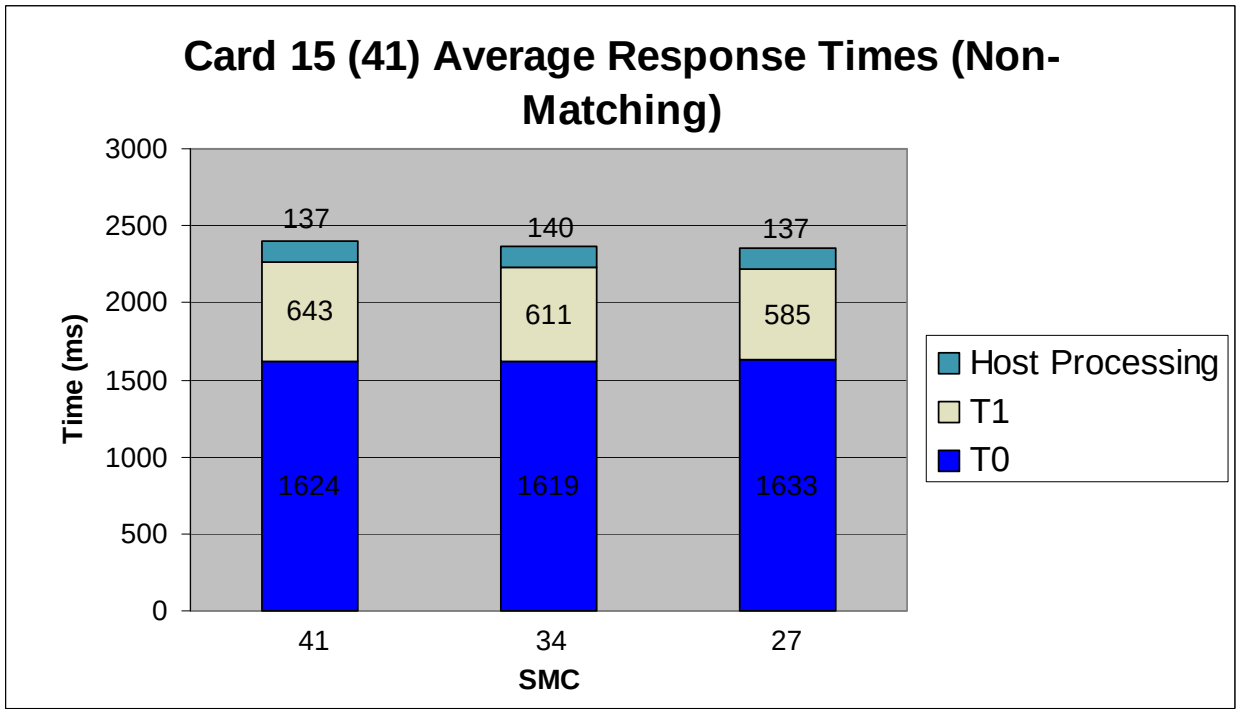


Figure B-70. Card 15 (41) Average Response Times for Non-Matching Templates

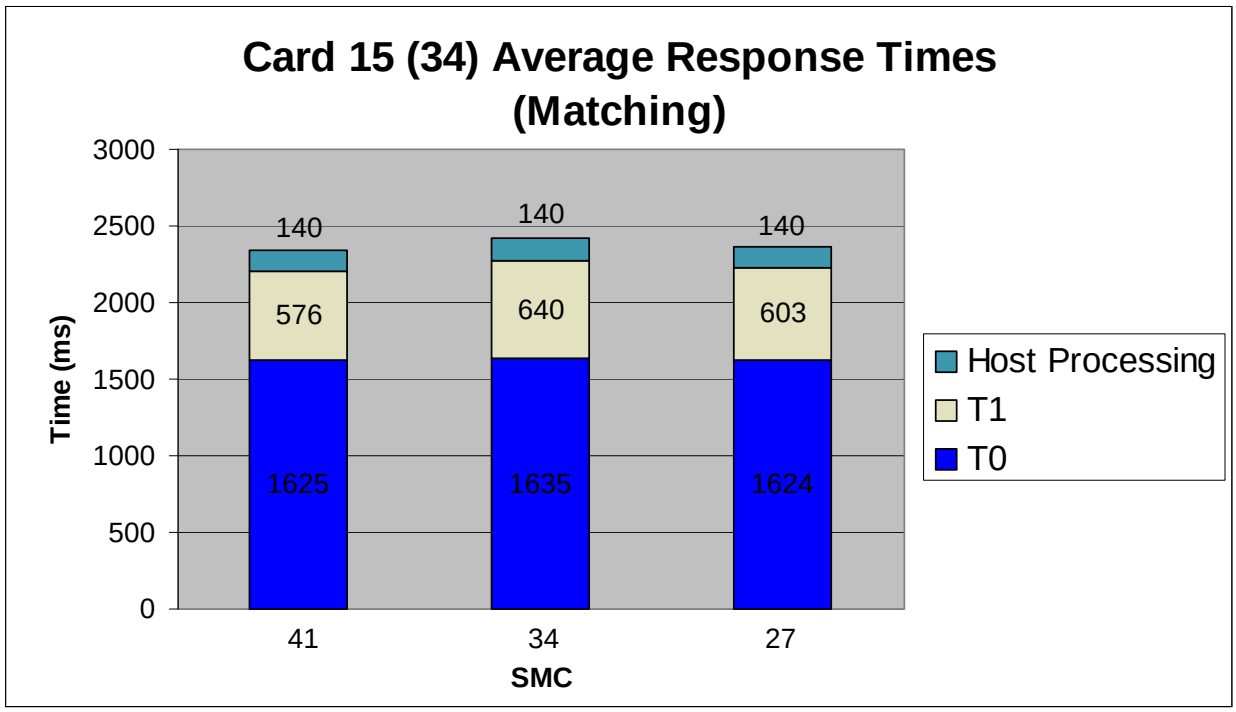


Figure B-71. Card 15 (34) Average Response Times for Matching Templates

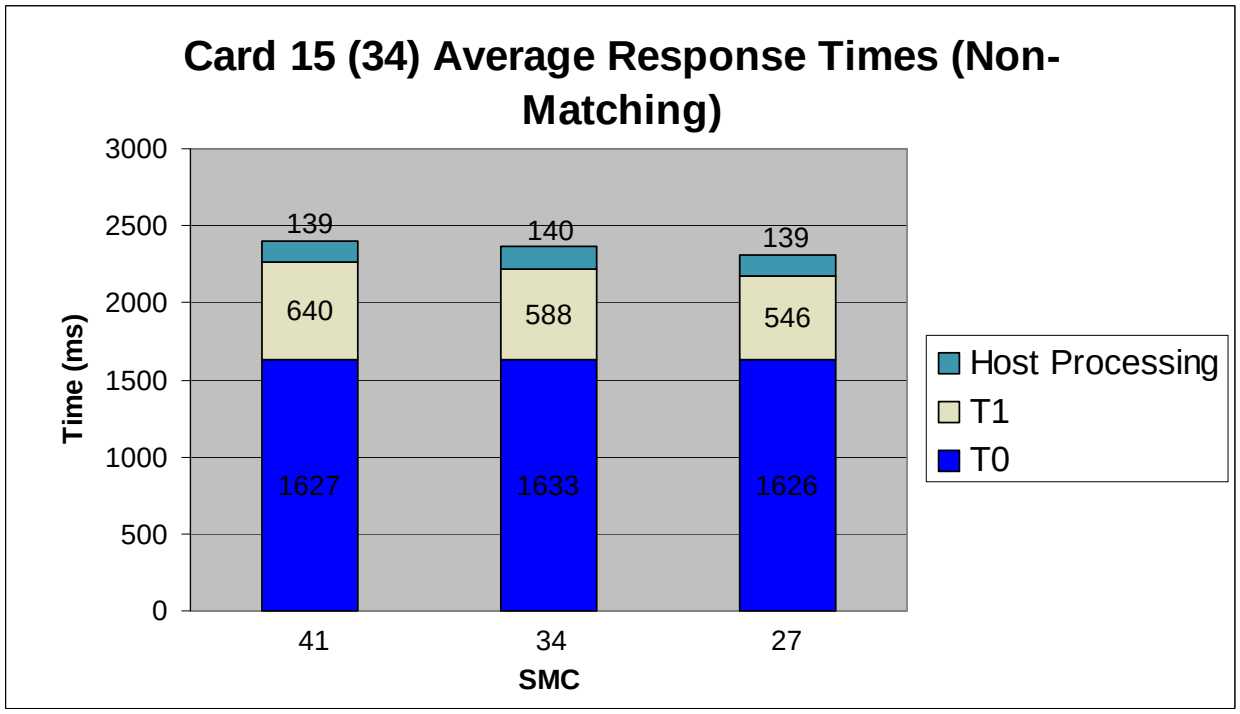


Figure B-72. Card 15 (34) Average Response Times for Non-Matching Templates

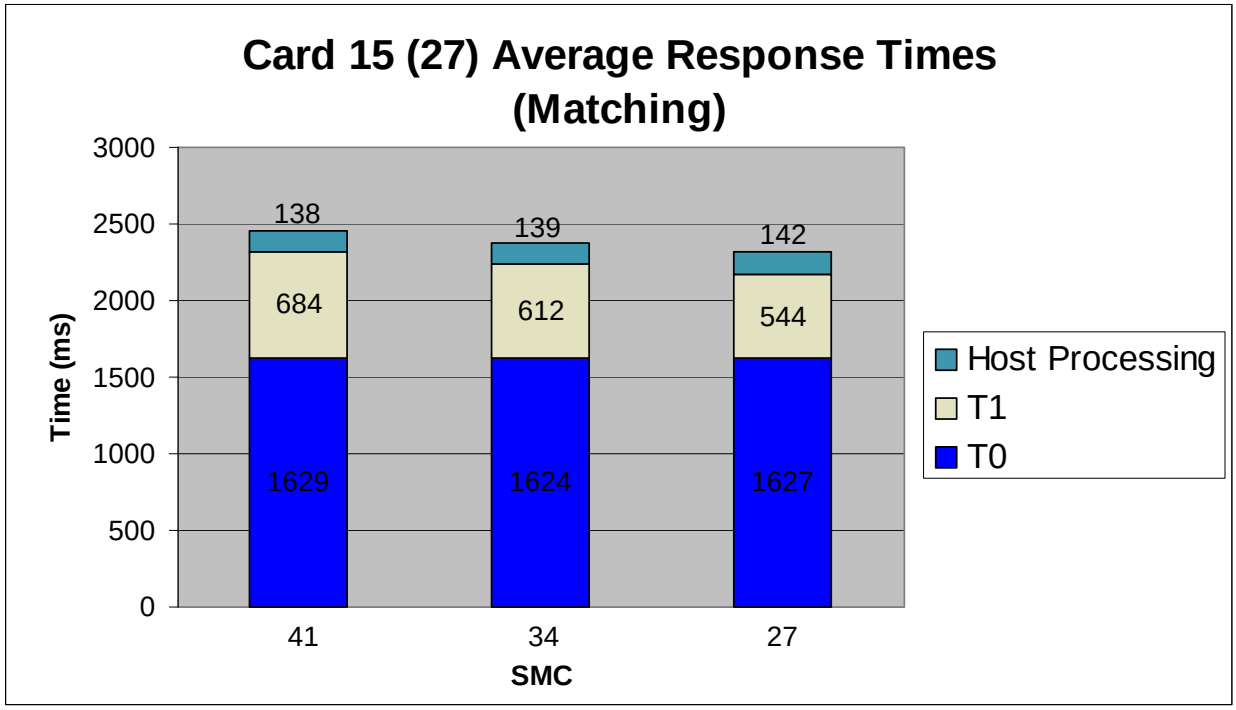


Figure B-73. Card 15 (27) Average Response Times for Matching Templates

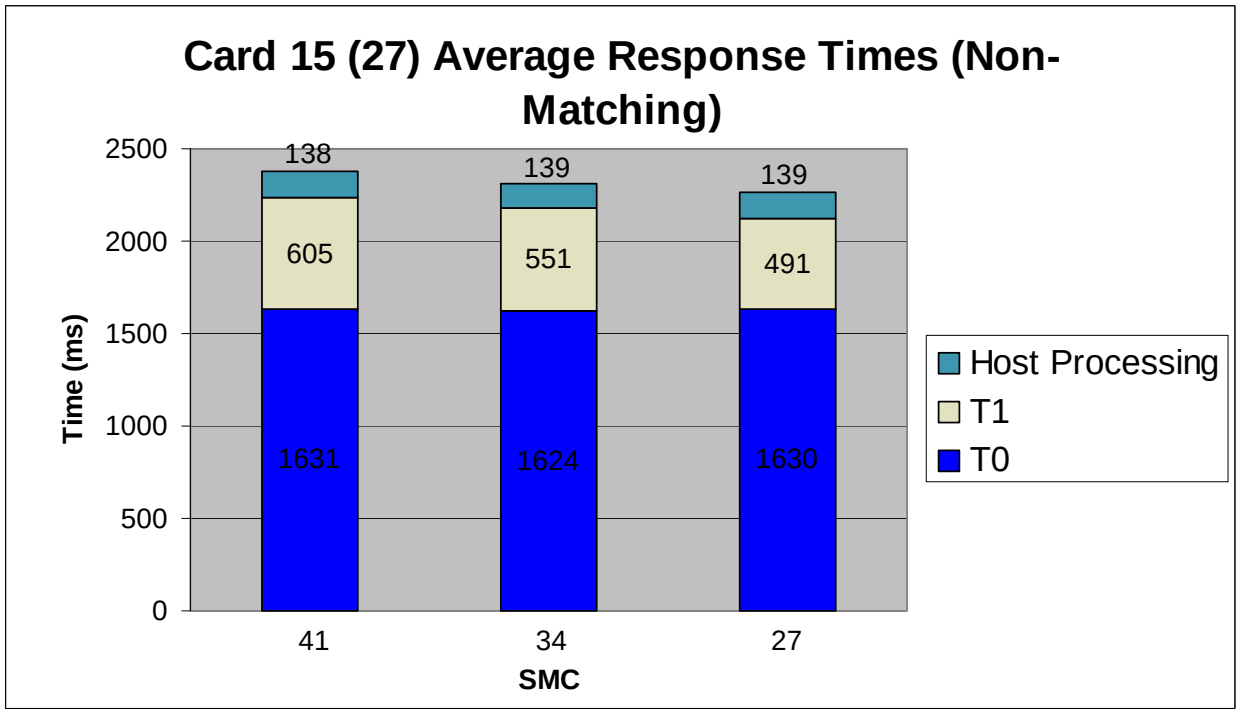


Figure B-74. Card 15 (27) Average Response Times for Non-Matching Templates

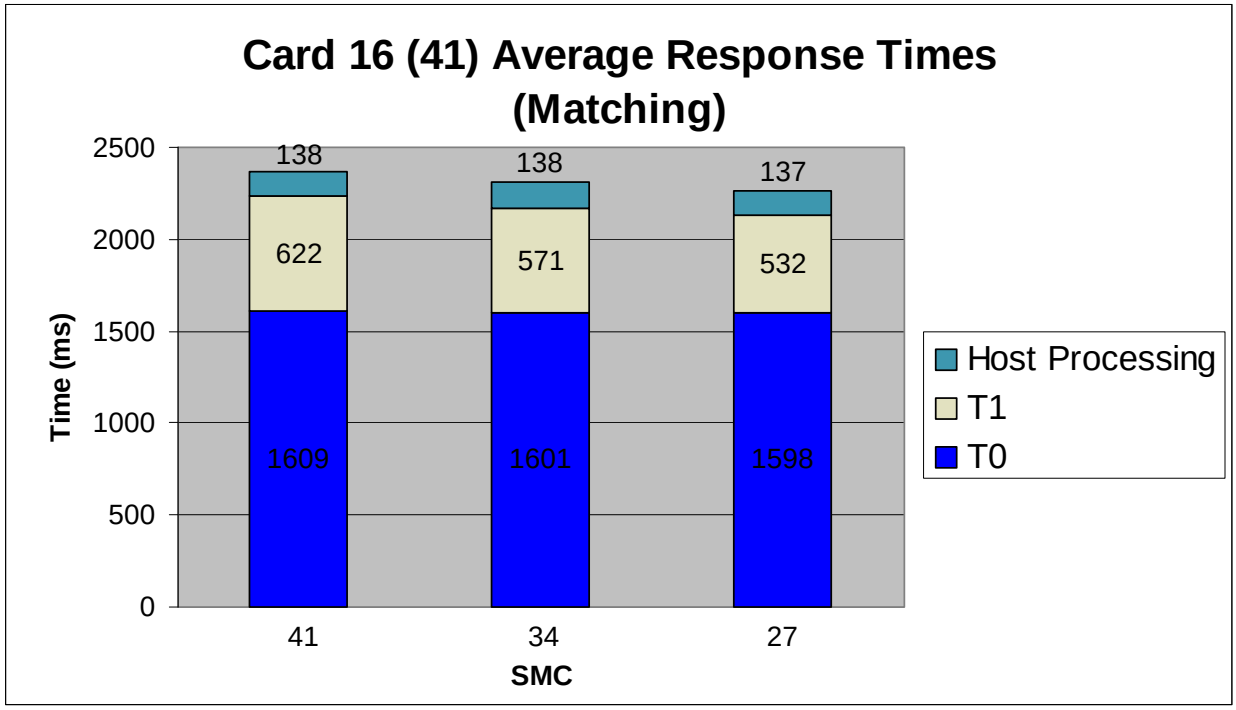


Figure B-75. Card 16 (41) Average Response Times for Matching Templates

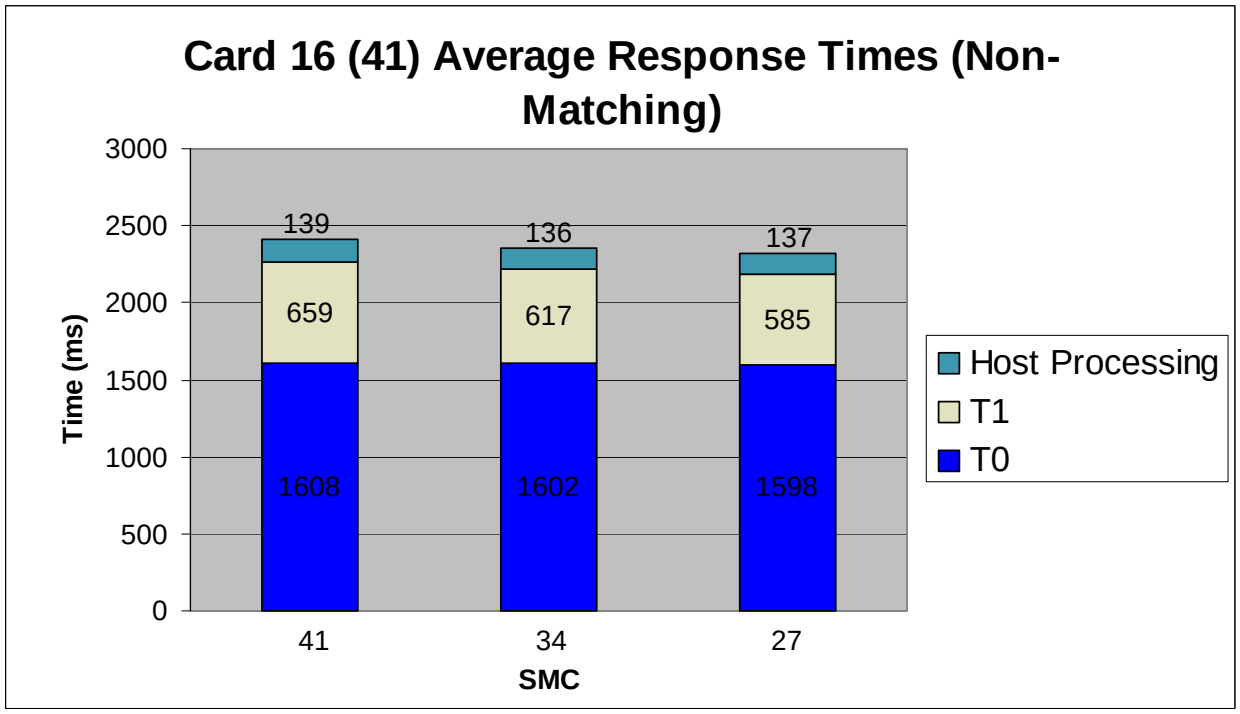


Figure B-76. Card 16 (41) Average Response Times for Non-Matching Templates

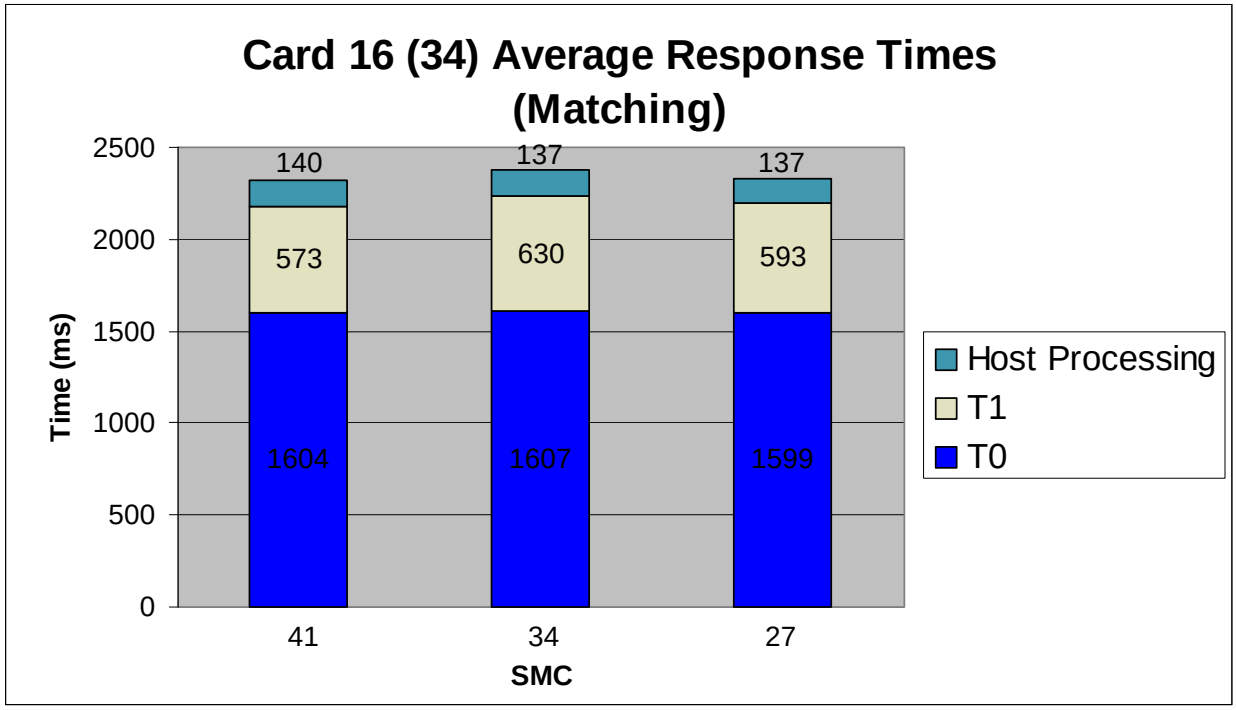


Figure B-77. Card 16 (34) Average Response Times for Matching Templates

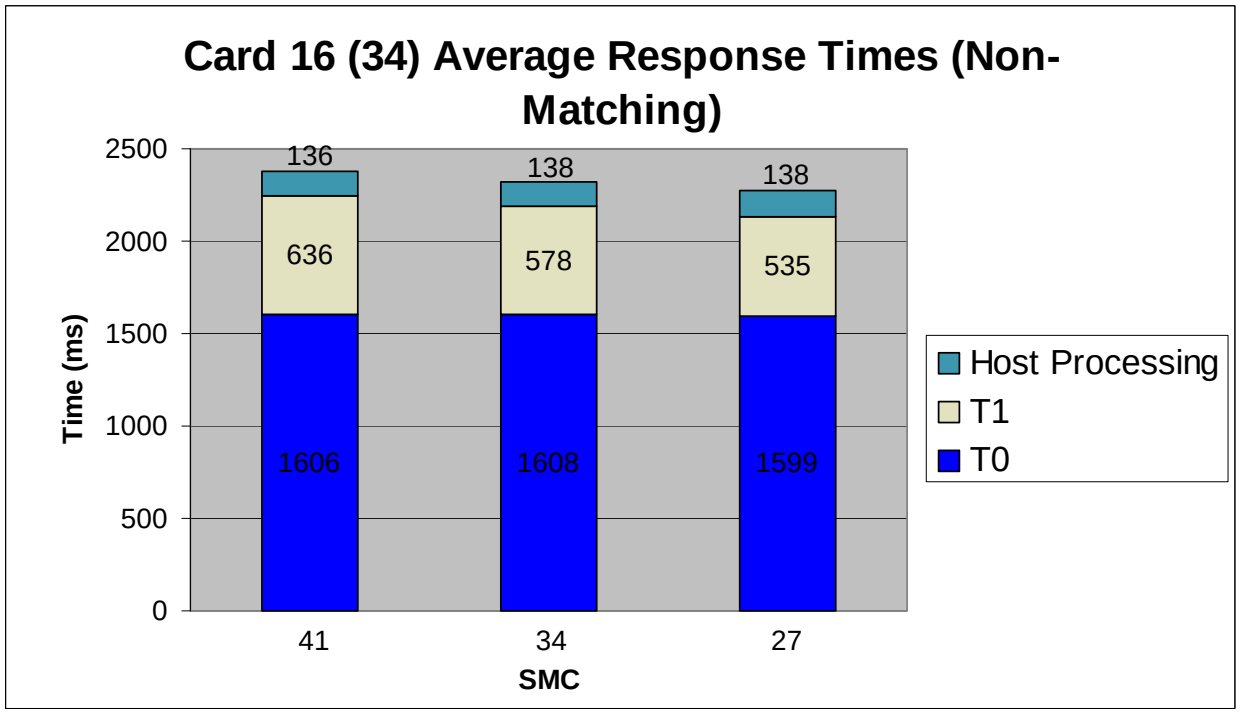


Figure B-78. Card 16 (34) Average Response Times for Non-Matching Templates

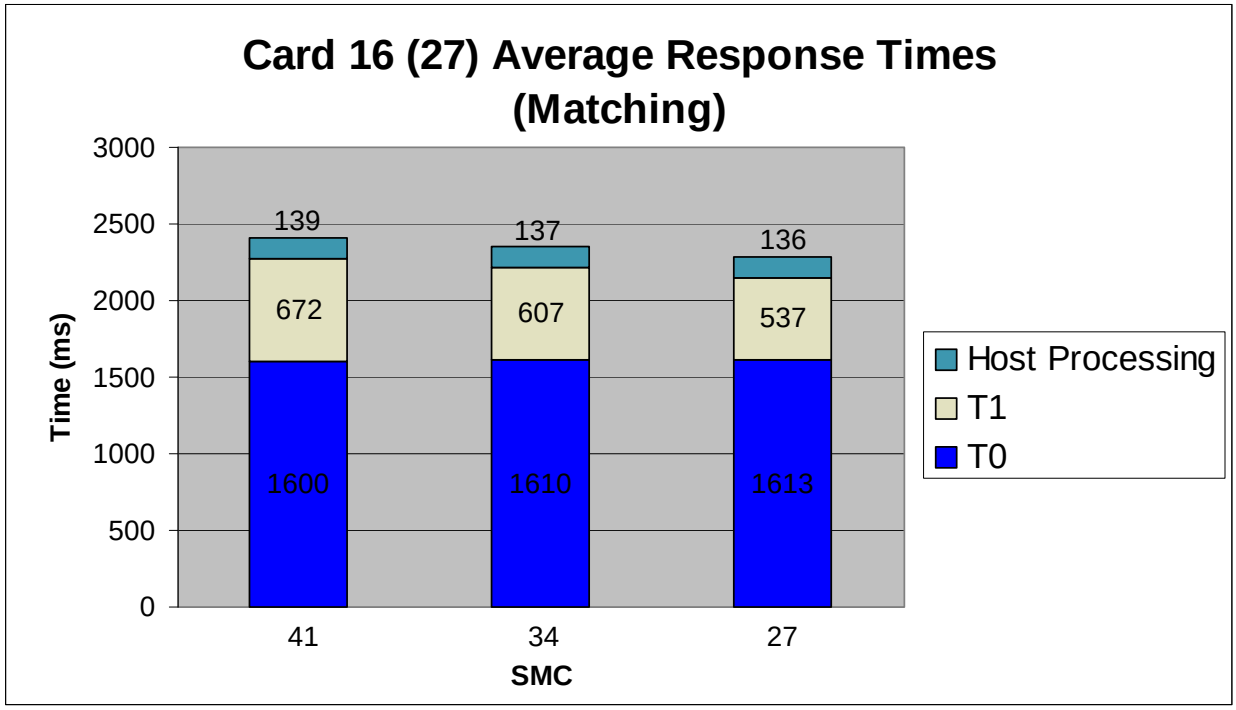


Figure B-79. Card 16 (27) Average Response Times for Matching Templates

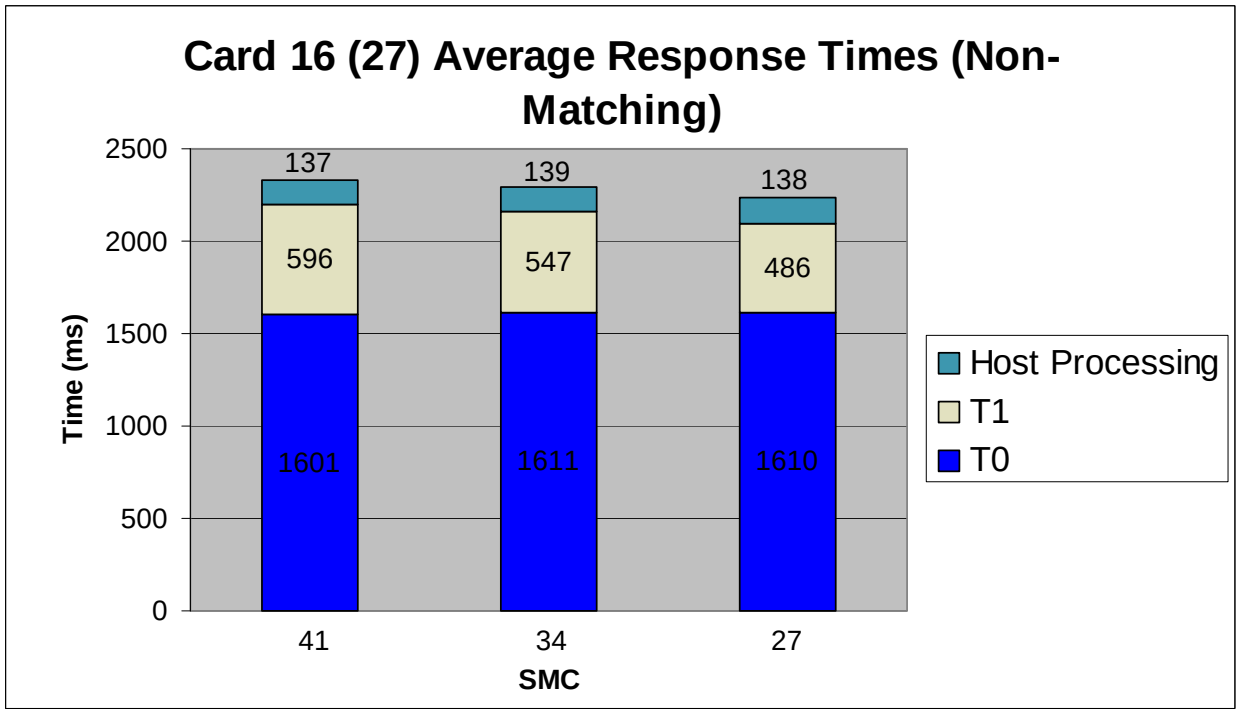


Figure B-80. Card 16 (27) Average Response Times for Non-Matching Templates

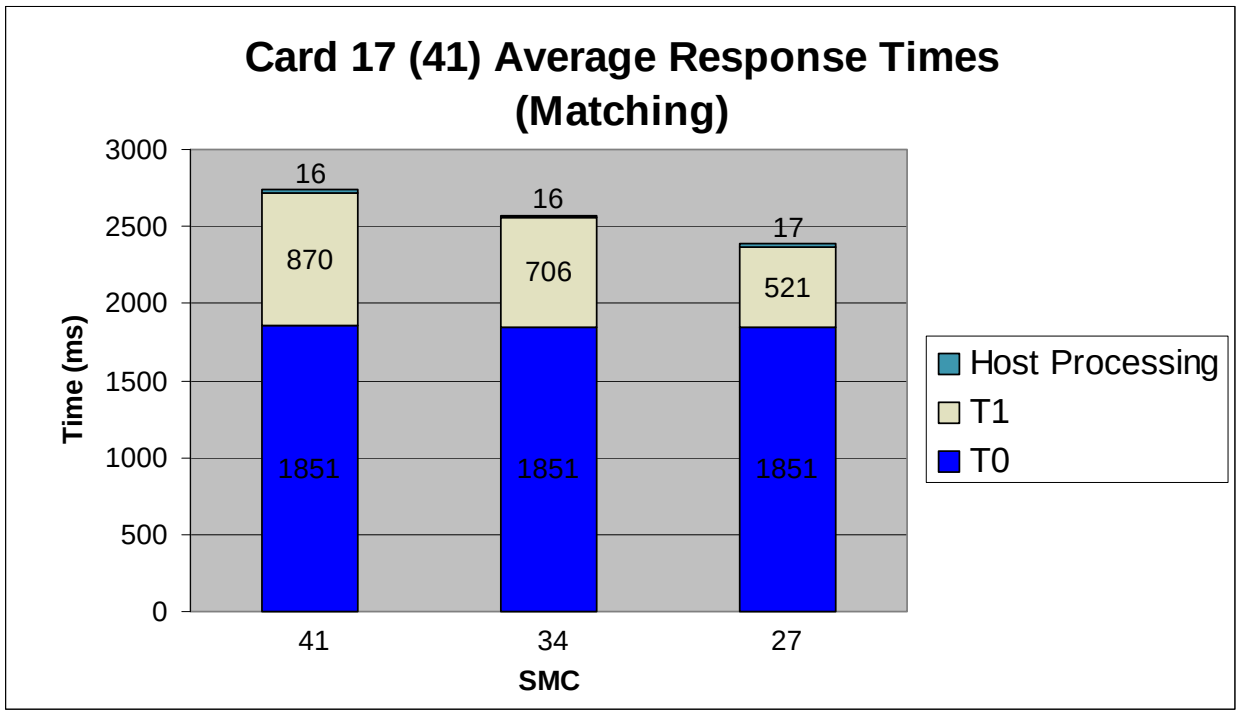


Figure B-81. Card 17 (41) Average Response Times for Matching Templates

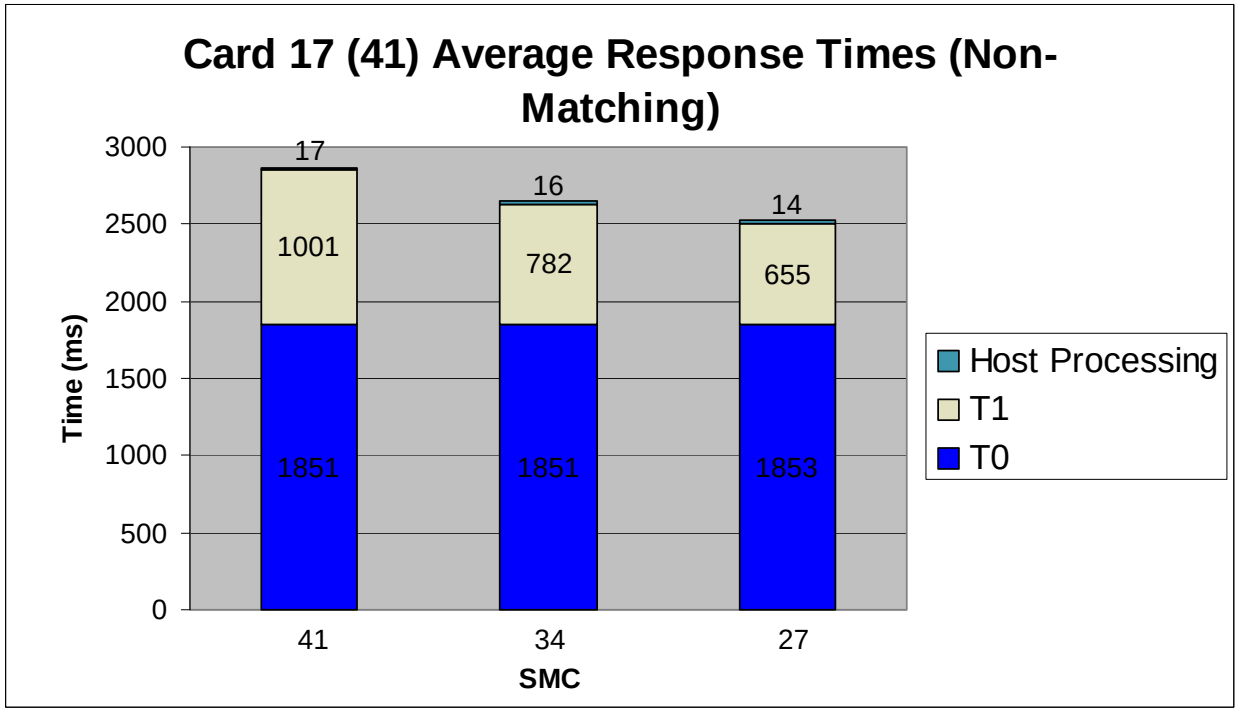


Figure B-82. Card 17 (41) Average Response Times for Non-Matching Templates

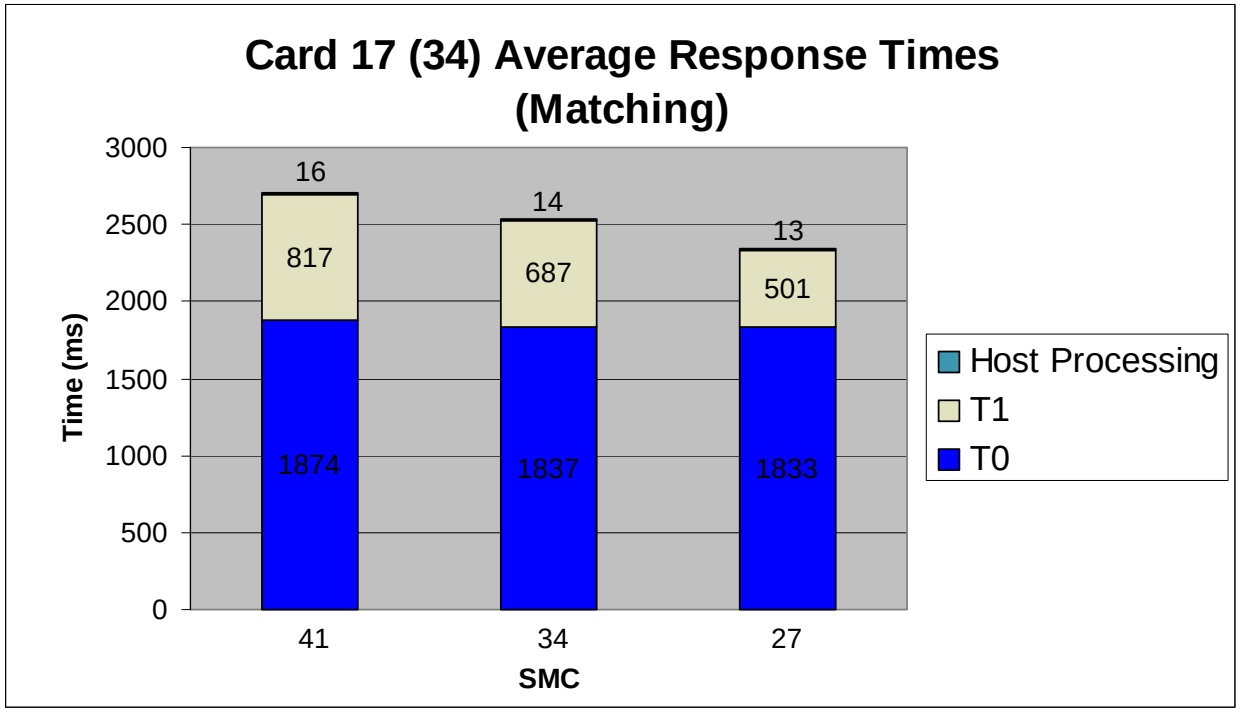


Figure B-83. Card 17 (34) Average Response Times for Matching Templates

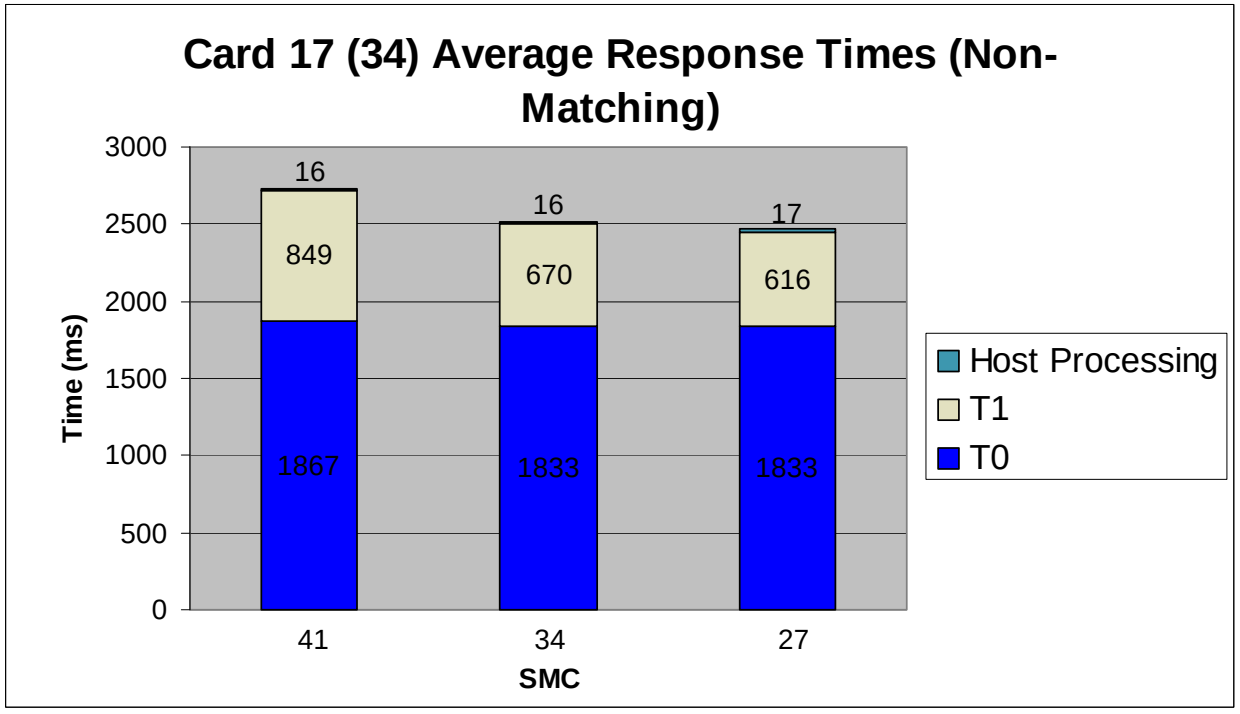


Figure B-84. Card 17 (34) Average Response Times for Non-Matching Templates

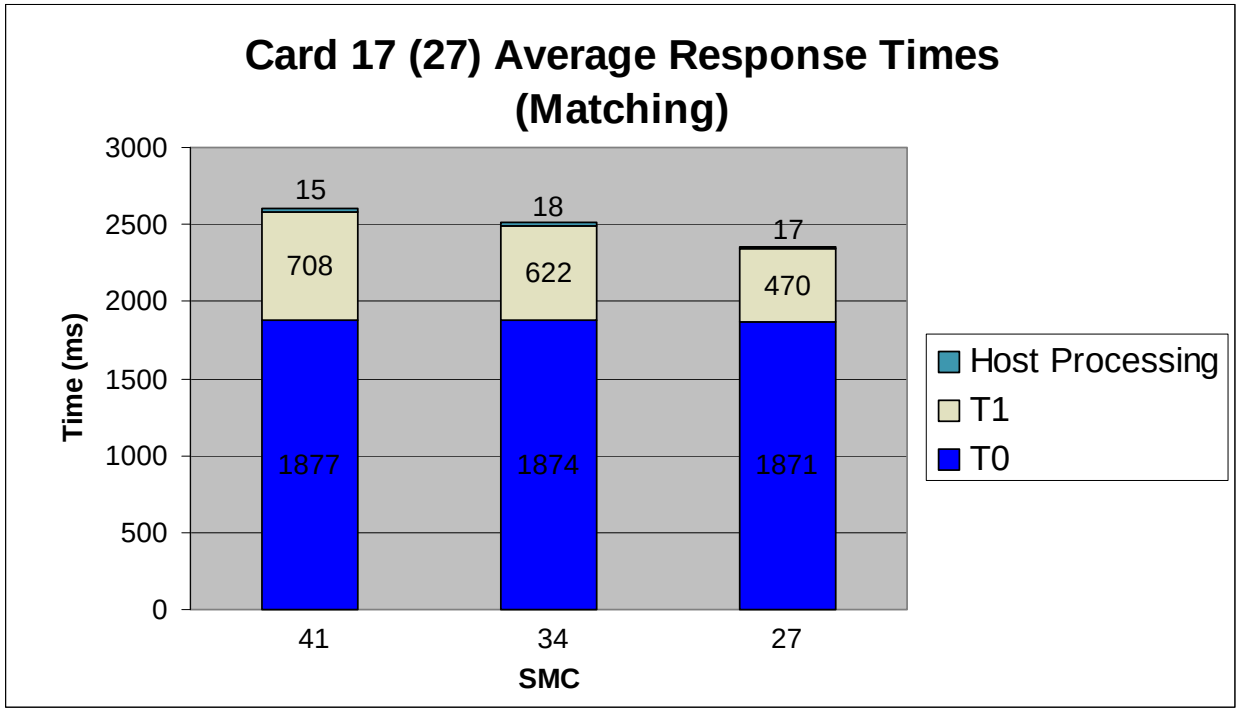


Figure B-85. Card 17 (27) Average Response Times for Matching Templates

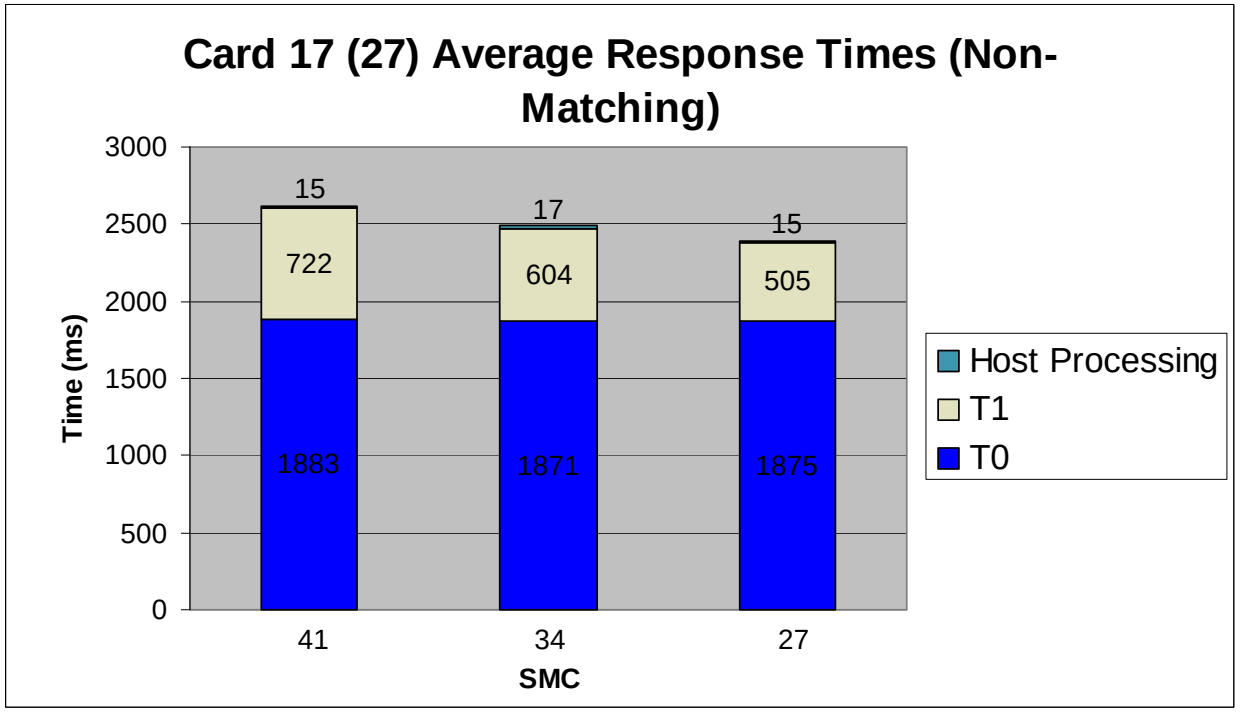


Figure B-86. Card 17 (27) Average Response Times for Non-Matching Templates

Appendix B—Response Time Graphs

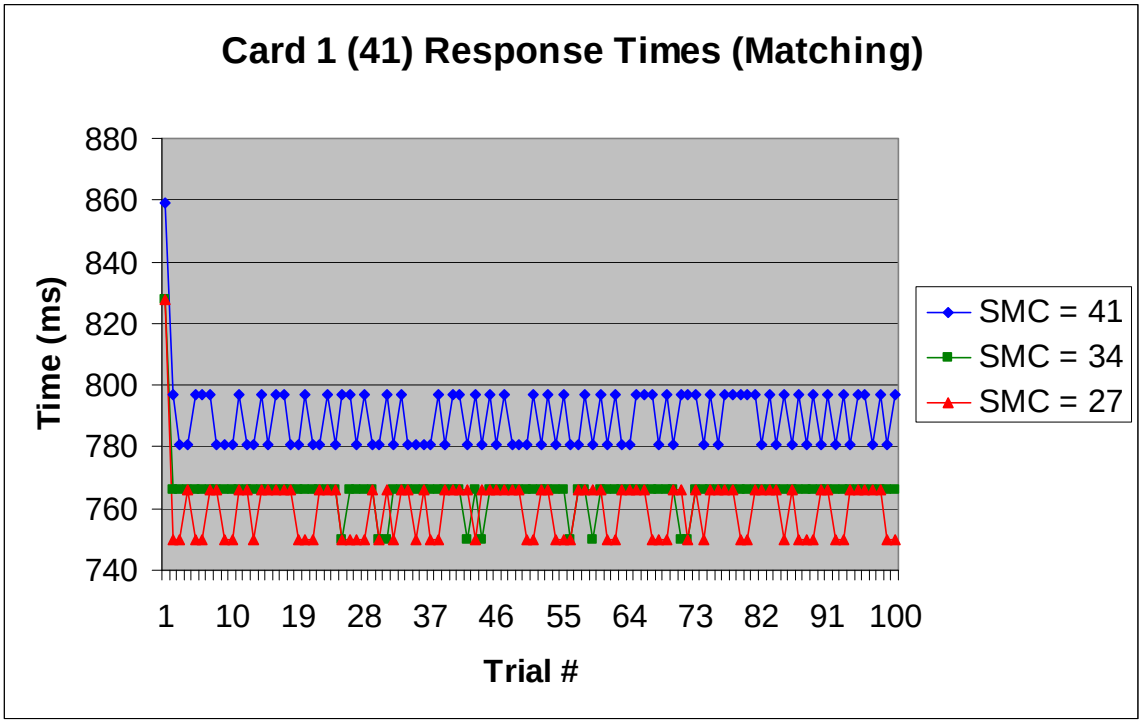


Figure C-1. Card 1 (41) Response Times for Matching Templates

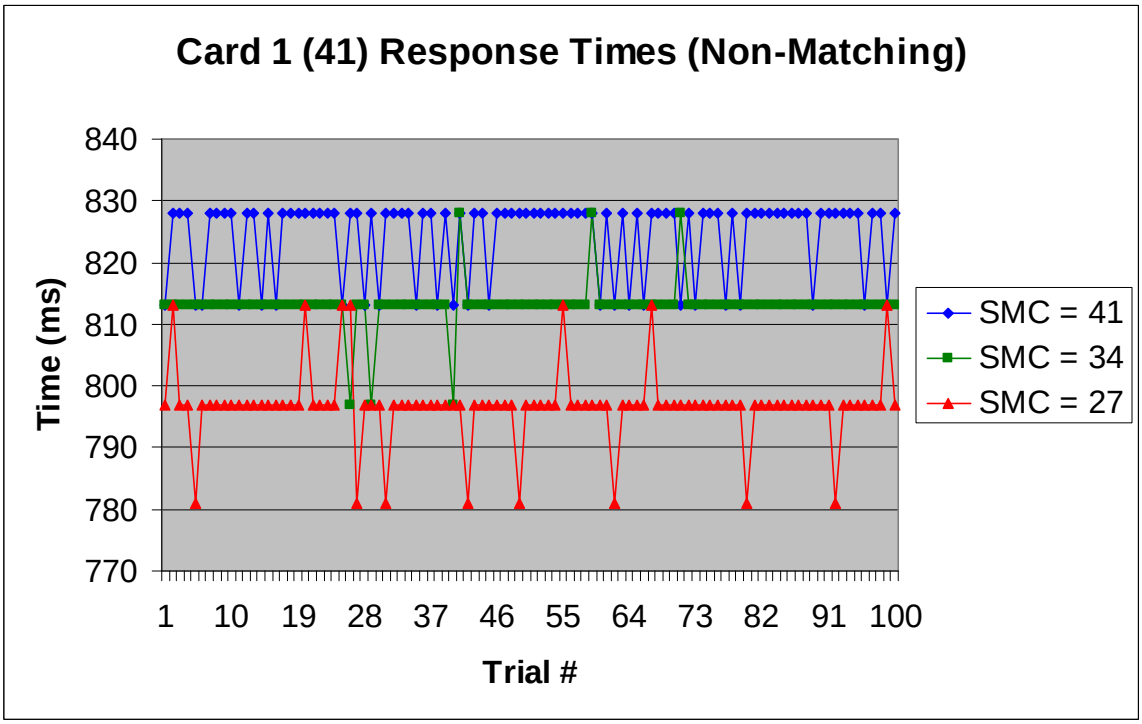


Figure C-2. Card 1 (41) Response Times for Non-Matching Templates

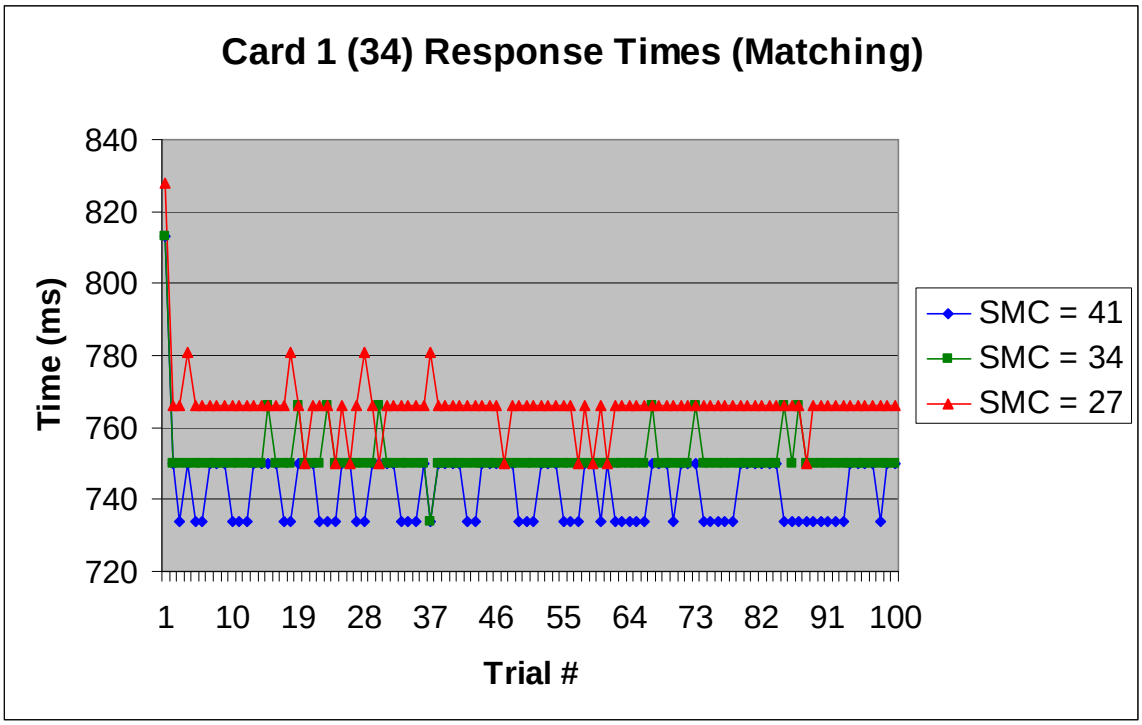


Figure C-3. Card 1 (34) Response Times for Matching Templates

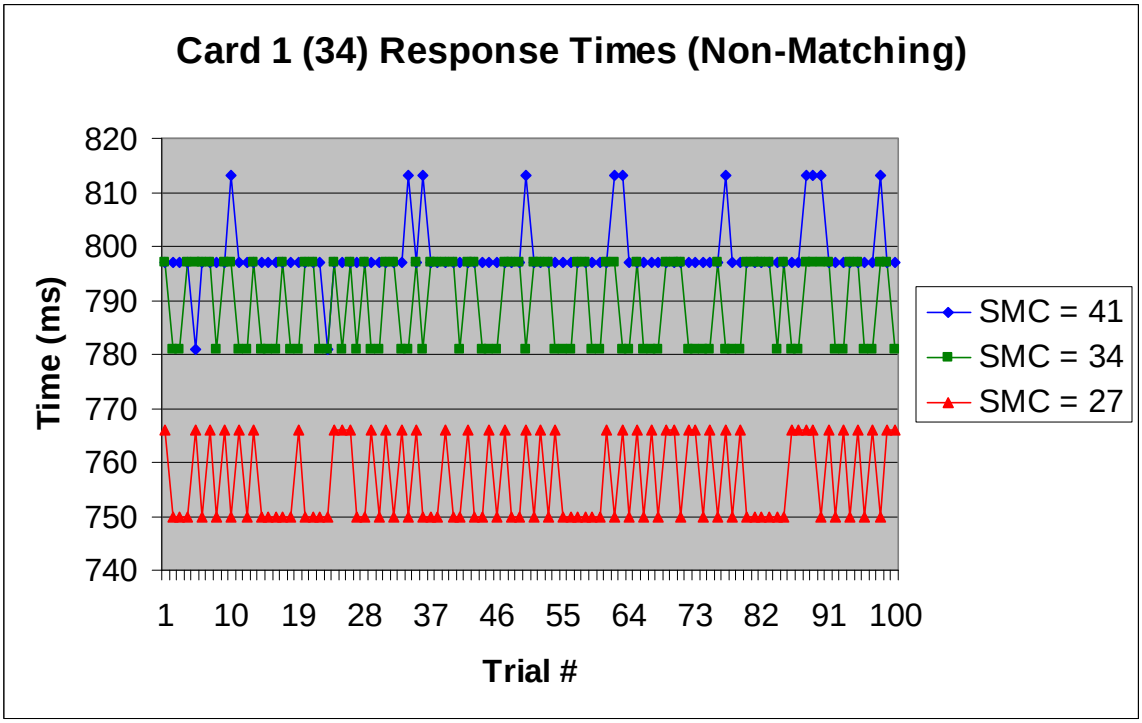


Figure C-4. Card 1 (34) Response Times for Non-Matching Templates

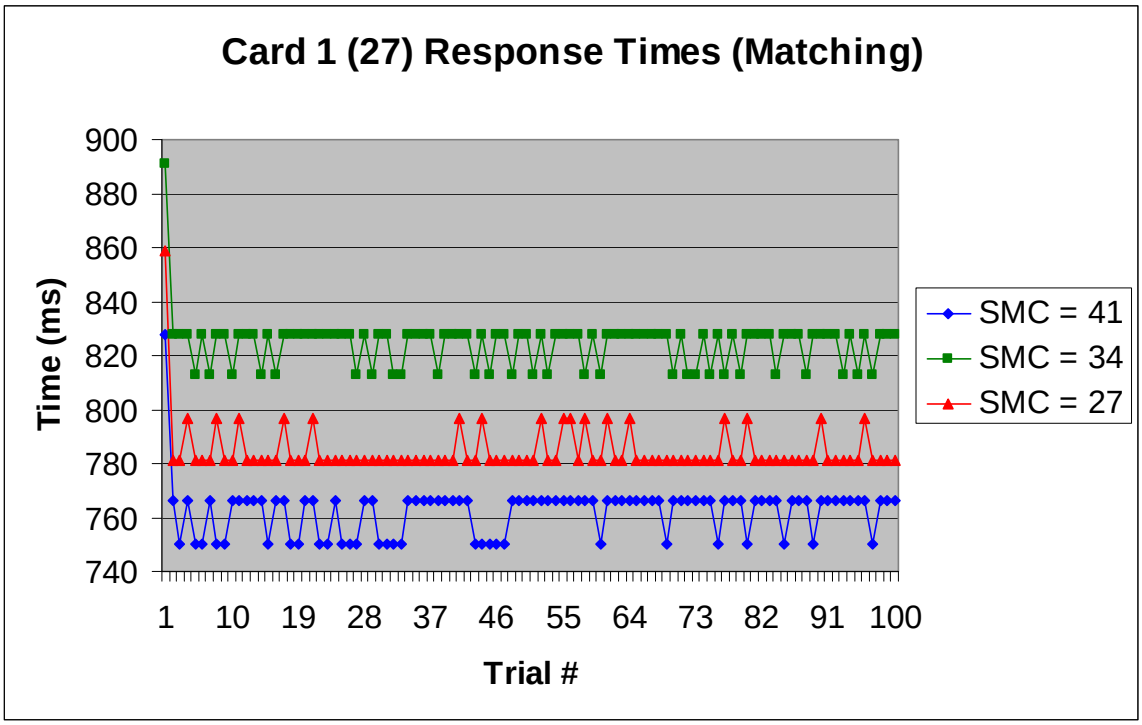


Figure C-5. Card 1 (27) Response Times for Matching Templates

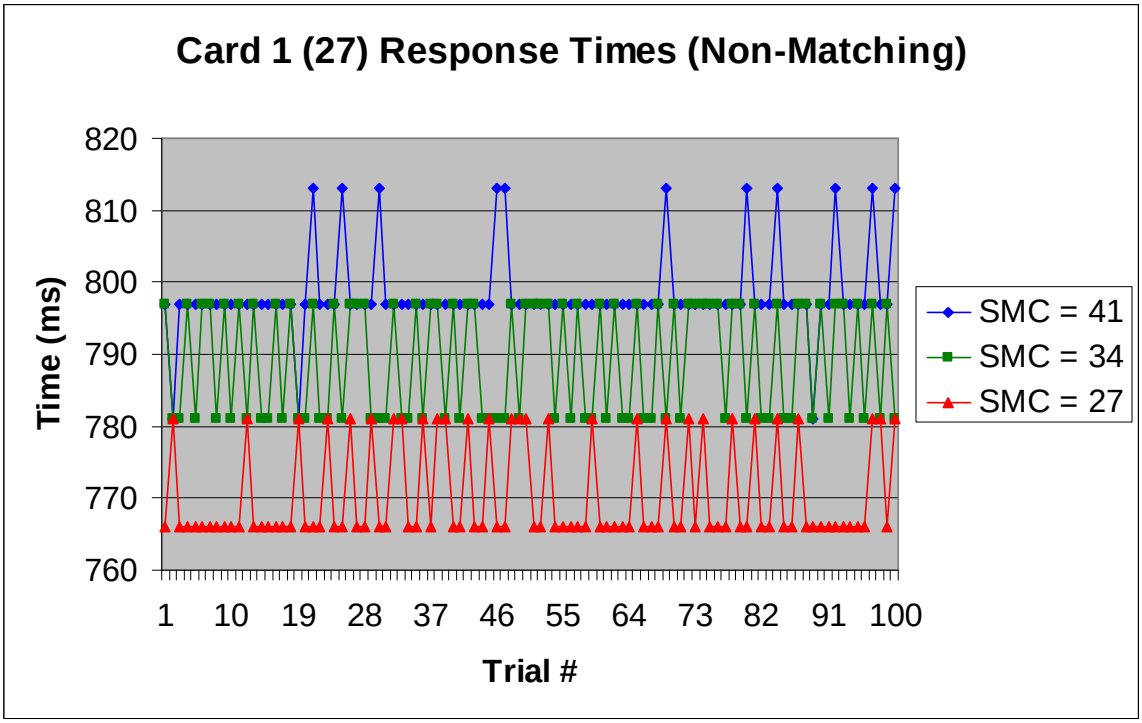


Figure C-6. Card 1 (27) Response Times for Non-Matching Templates

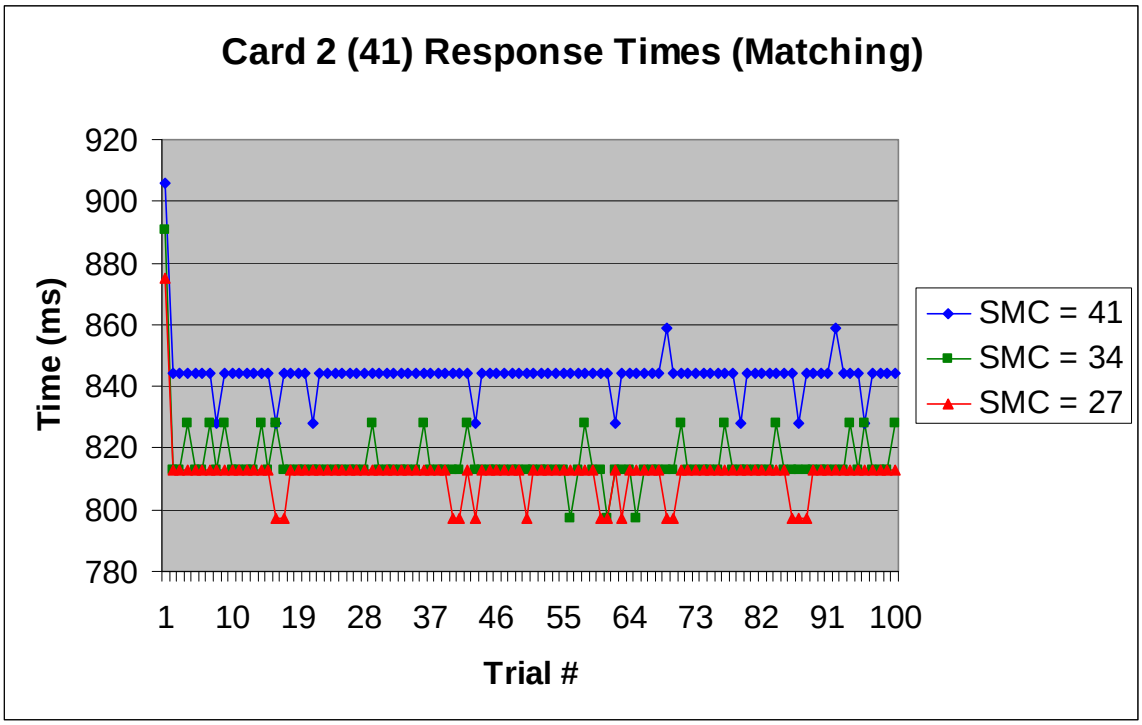


Figure C-7. Card 2 (41) Response Times for Matching Templates

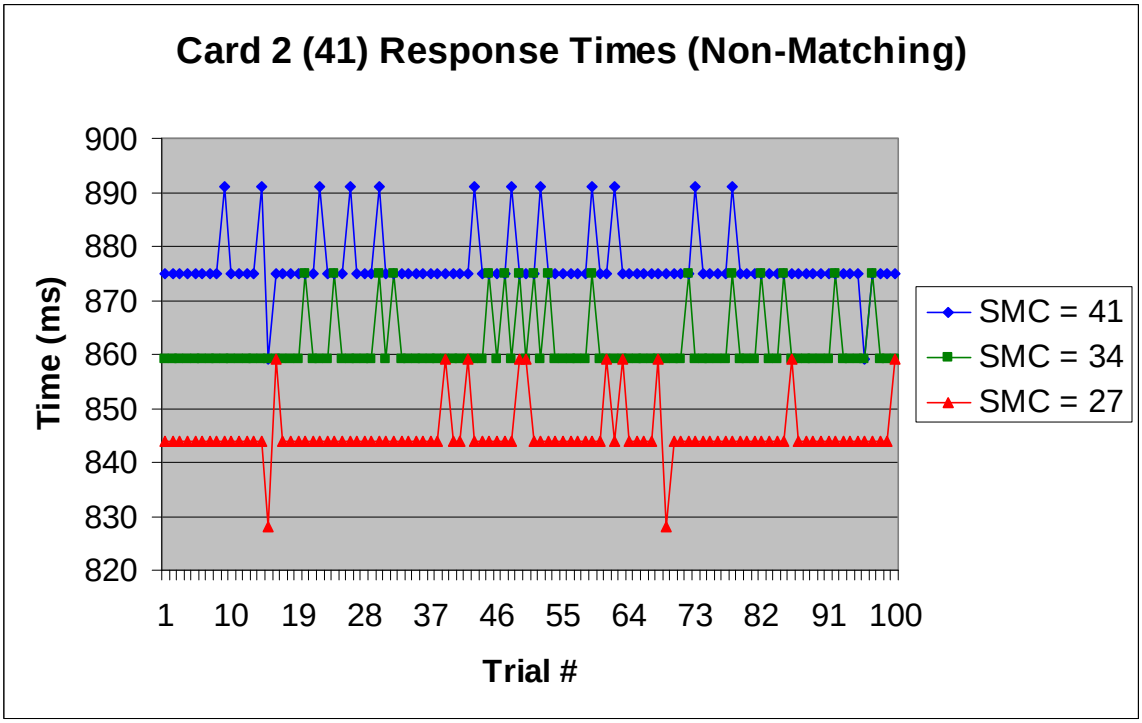


Figure C-8. Card 2 (41) Response Times for Non-Matching Templates

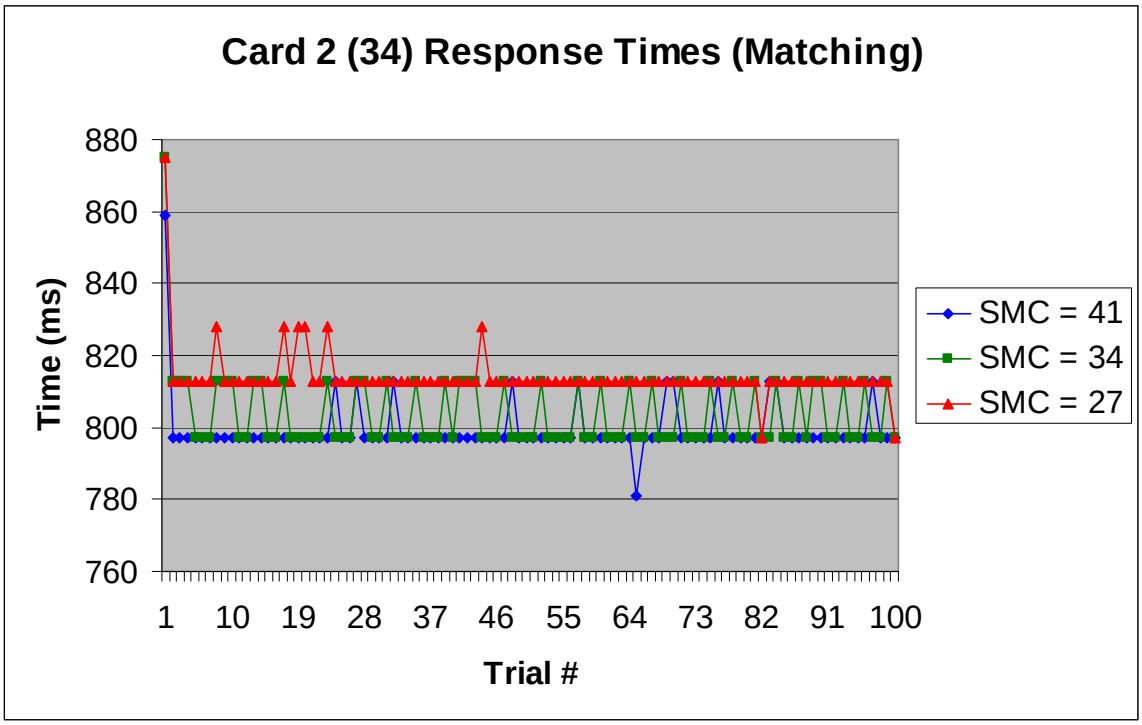


Figure C-9. Card 2 (34) Response Times for Matching Templates

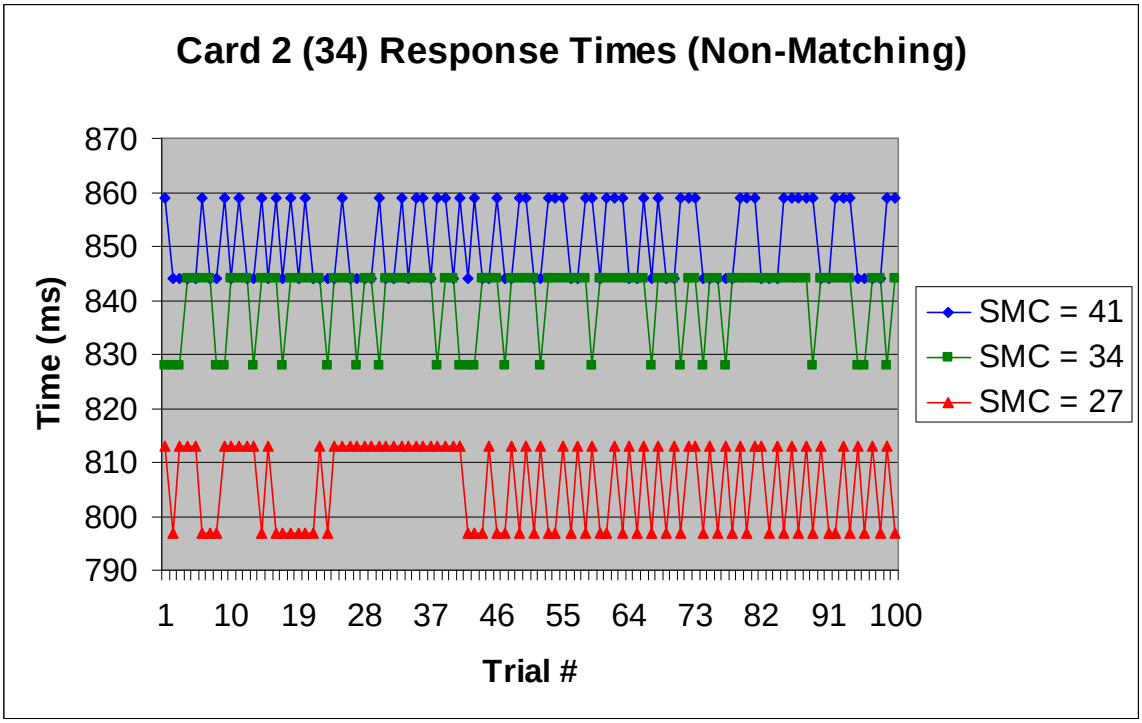


Figure C-10. Card 2 (34) Response Times for Non-Matching Templates

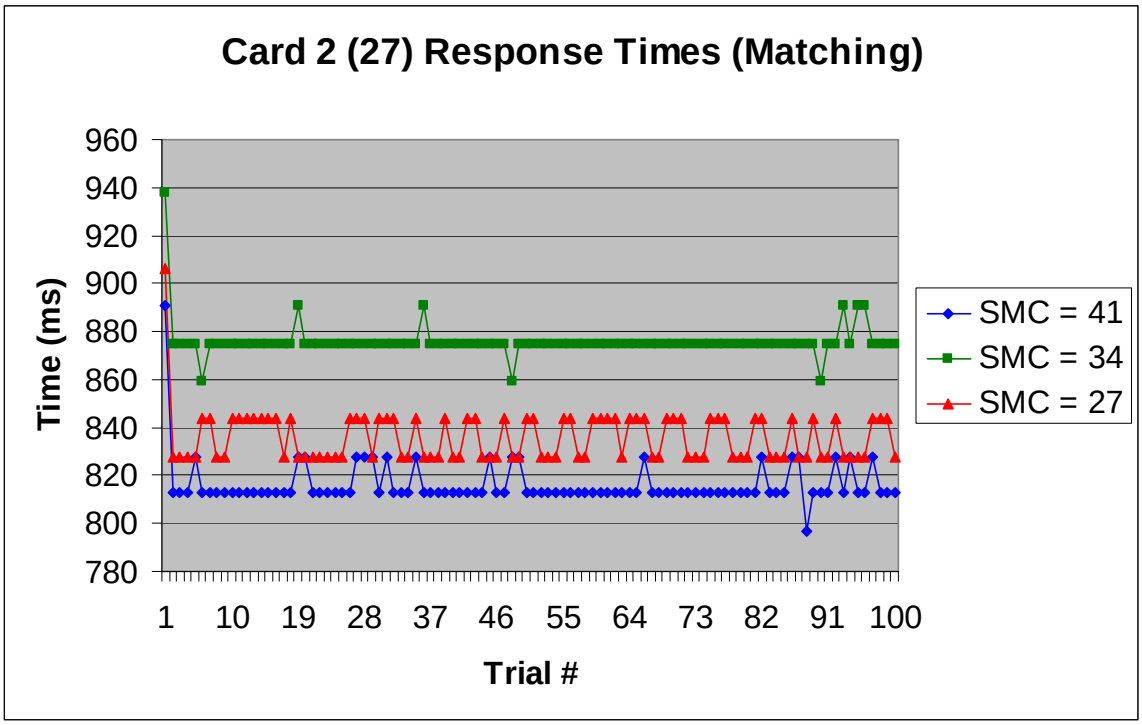


Figure C-11. Card 2 (27) Response Times for Matching Templates

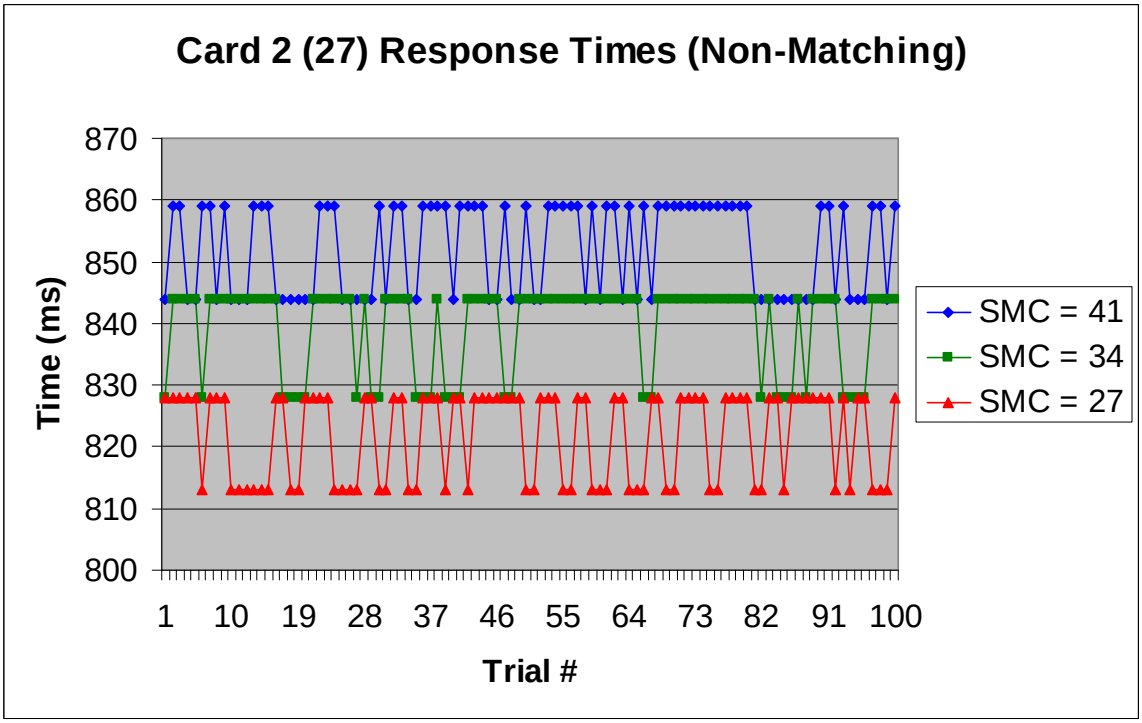


Figure C-12. Card 2 (27) Response Times for Non-Matching Templates

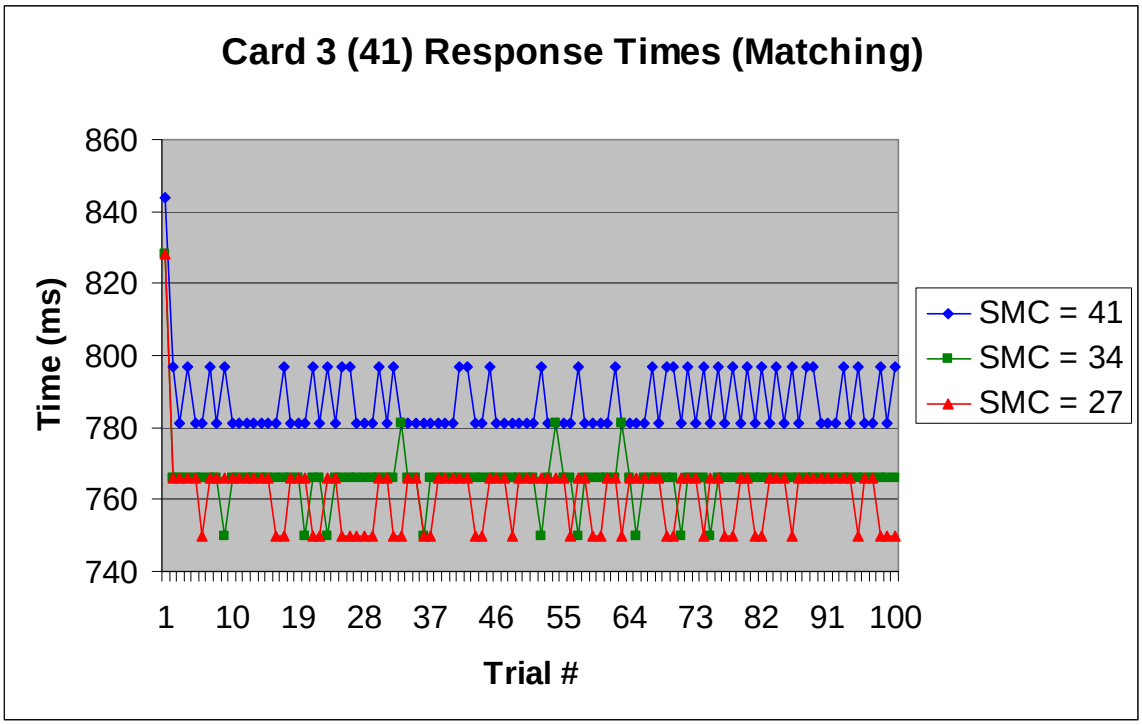


Figure C-13. Card 3 (41) Response Times for Matching Templates[7]

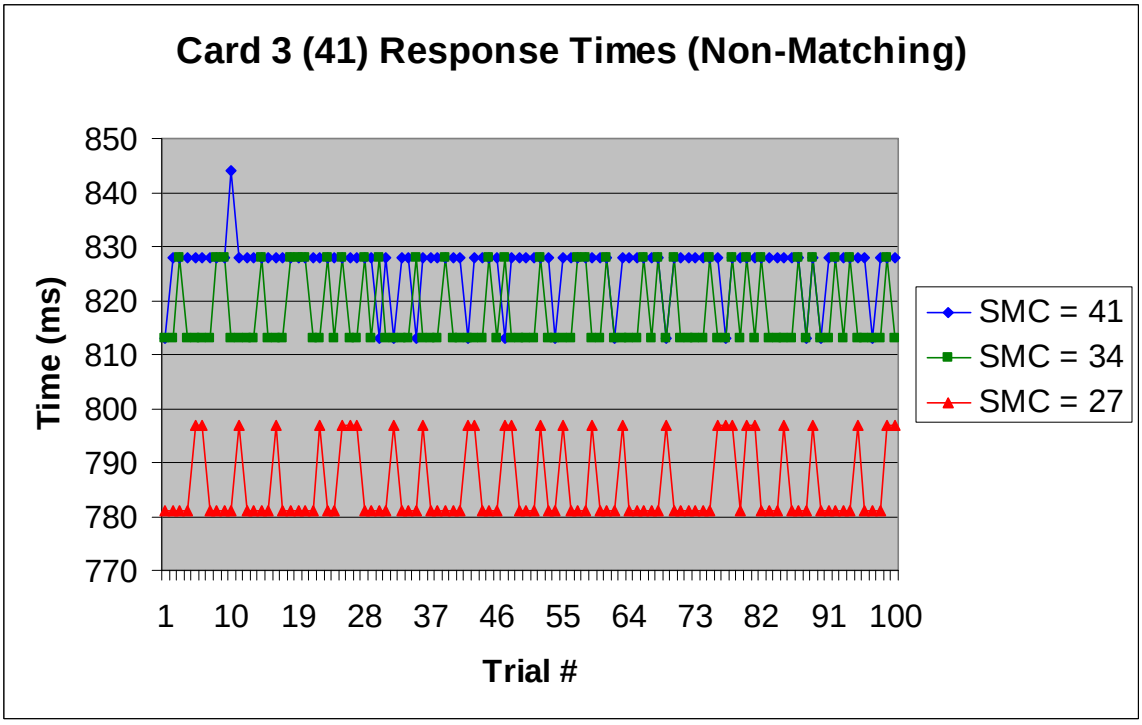


Figure C-14. Card 3 (41) Response Times for Non-Matching Templates

[7] Card 3 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

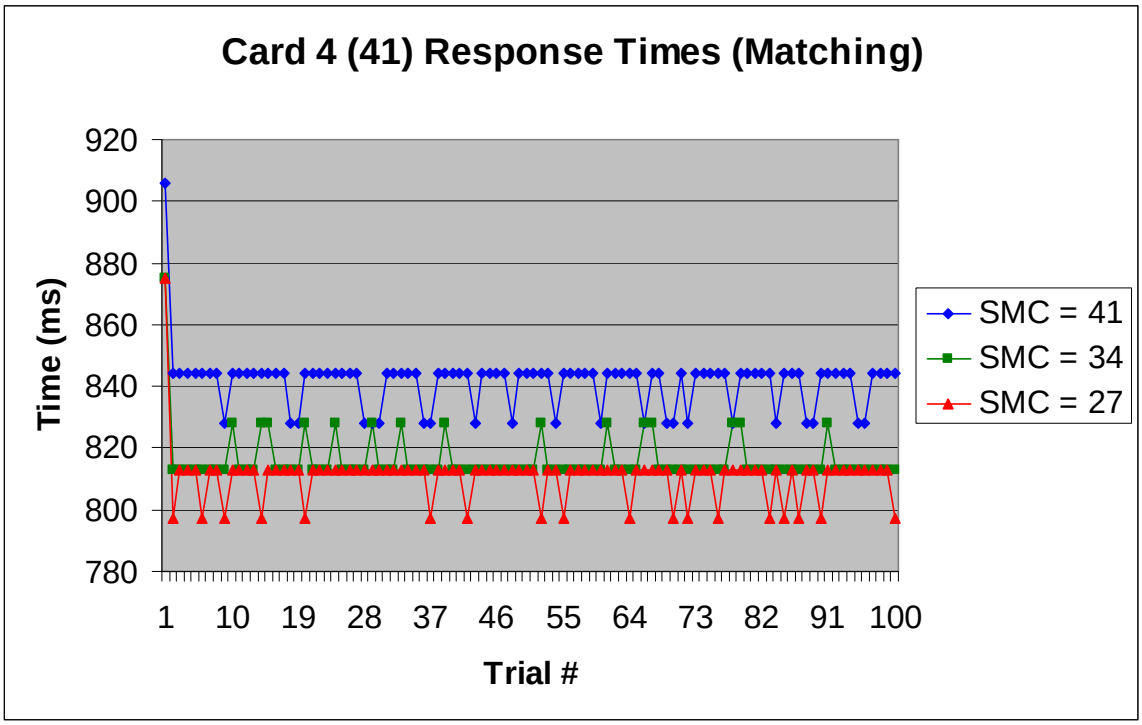


Figure C-15. Card 4 (41) Response Times for Matching Templates[8]

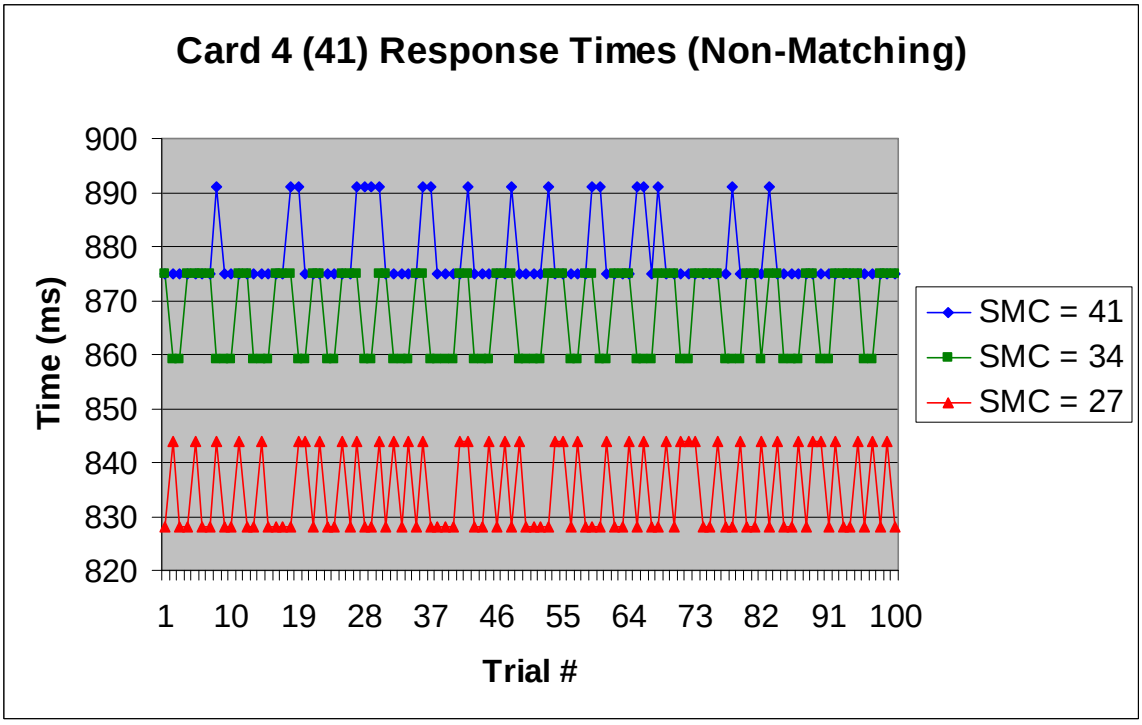


Figure C-16. Card 4 (41) Response Times for Non-Matching Templates

[8] Card 4 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

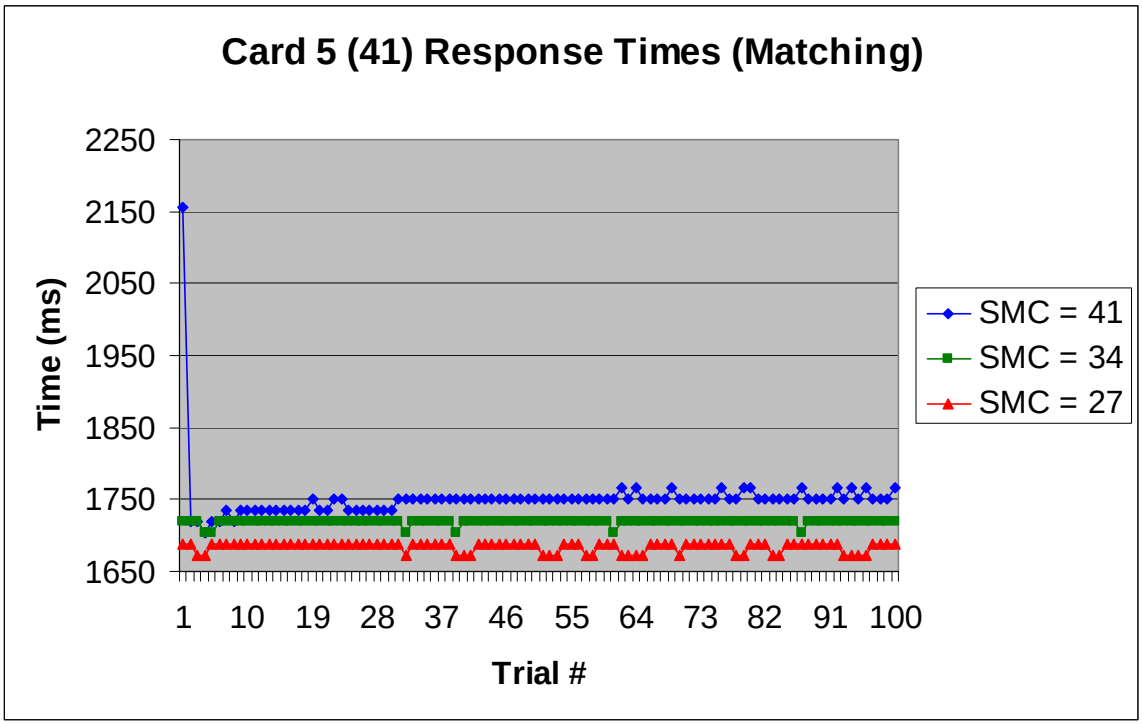


Figure C-17. Card 5 (41) Response Times for Matching Templates

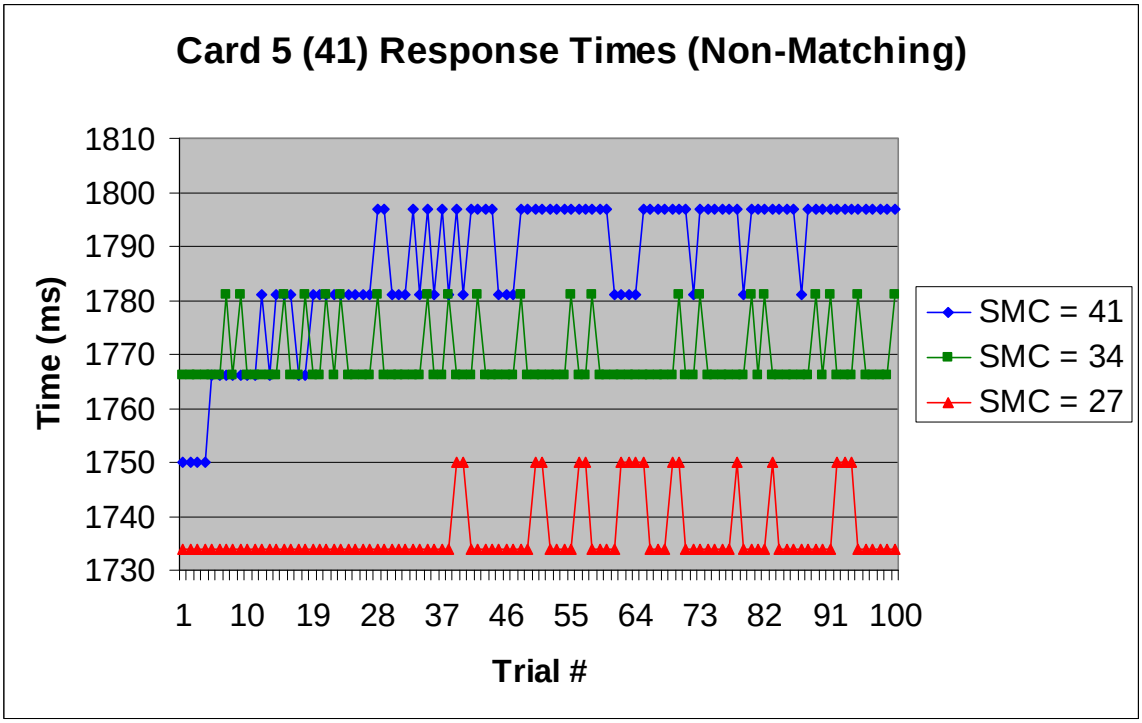


Figure C-18. Card 5 (41) Response Times for Non-Matching Templates

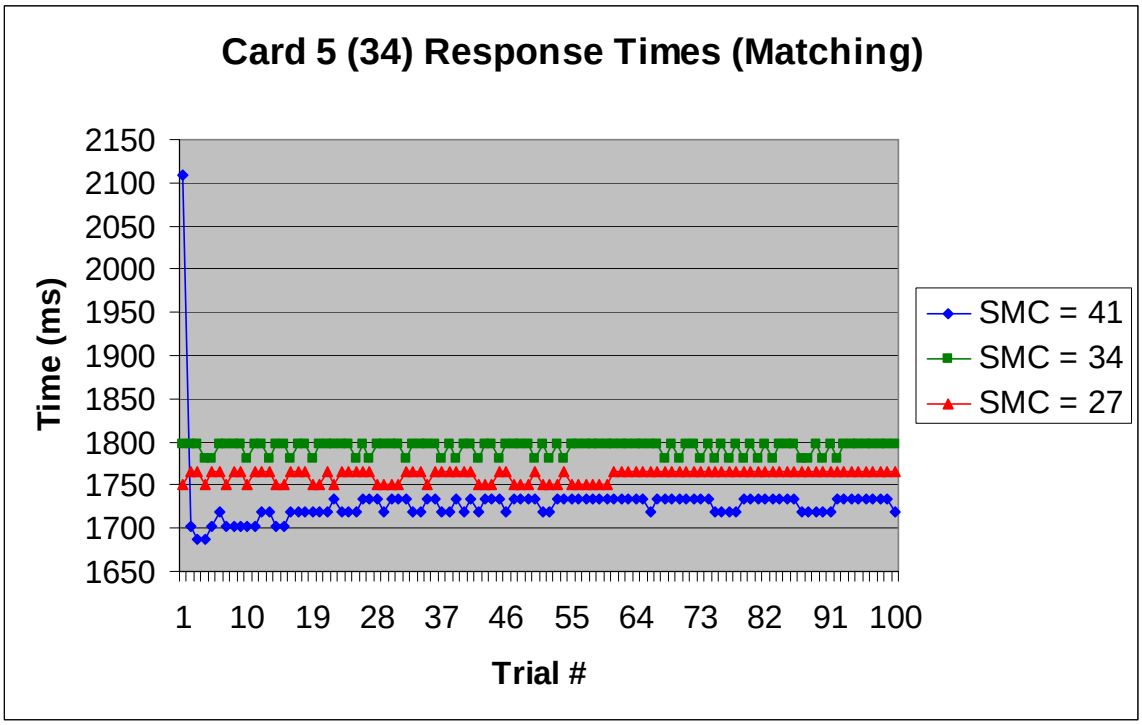


Figure C-19. Card 5 (34) Response Times for Matching Templates

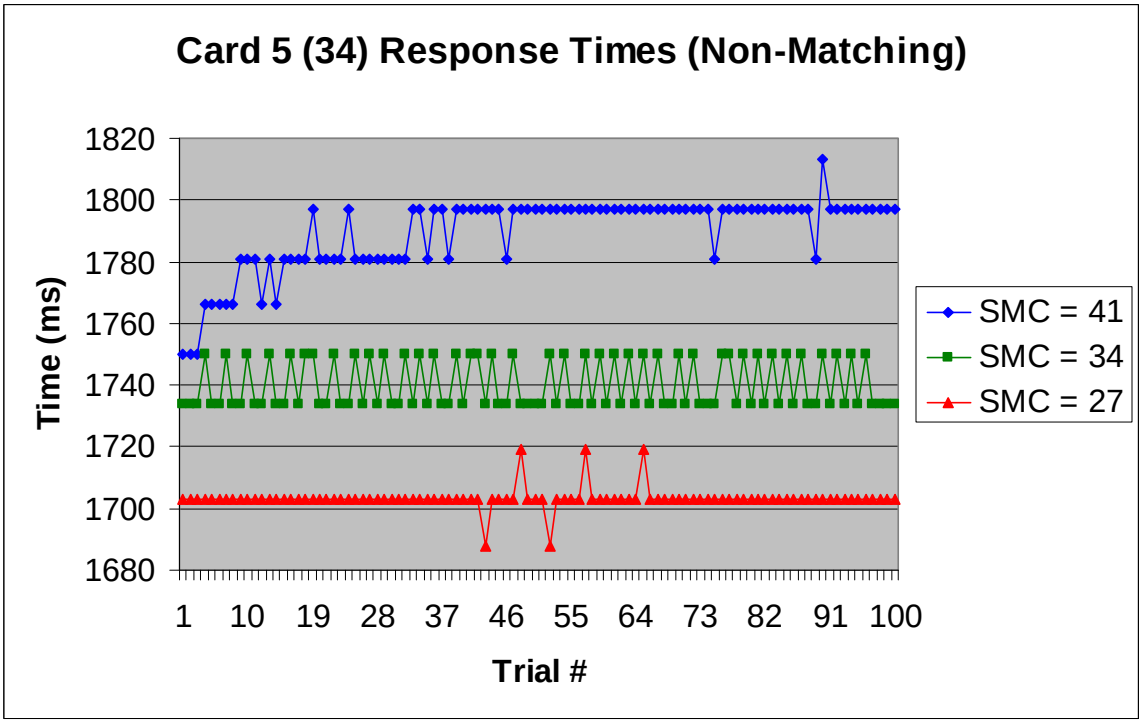


Figure C-20. Card 5 (34) Response Times for Non-Matching Templates

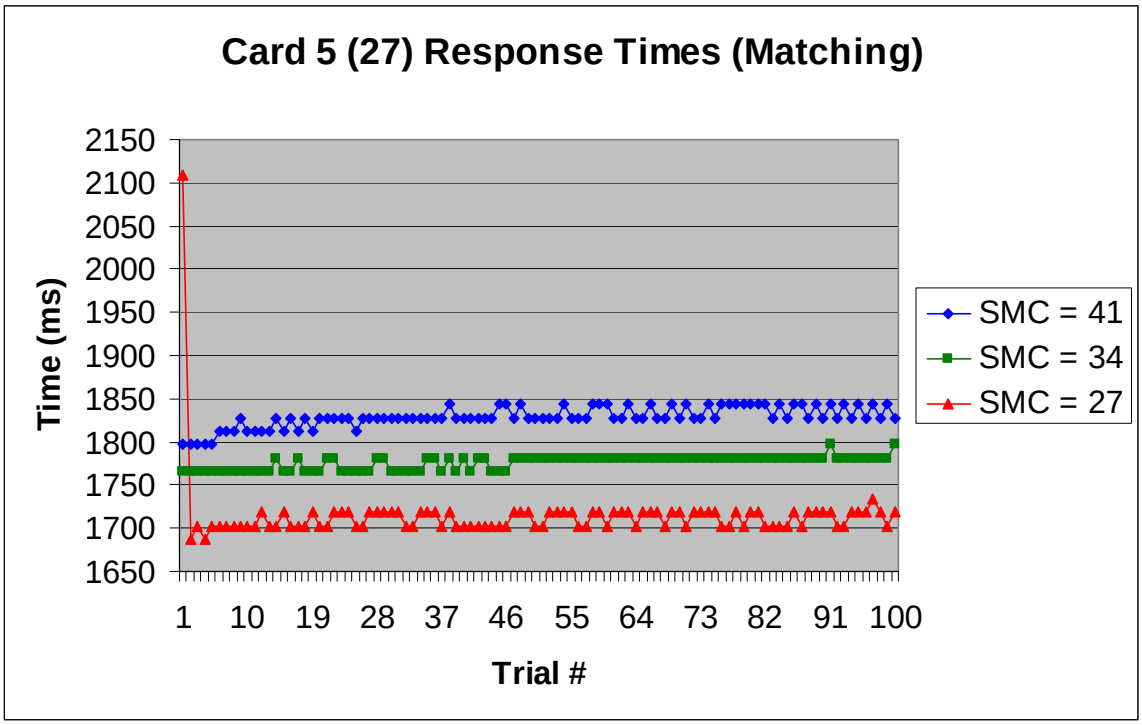


Figure C-21. Card 5 (27) Response Times for Matching Templates

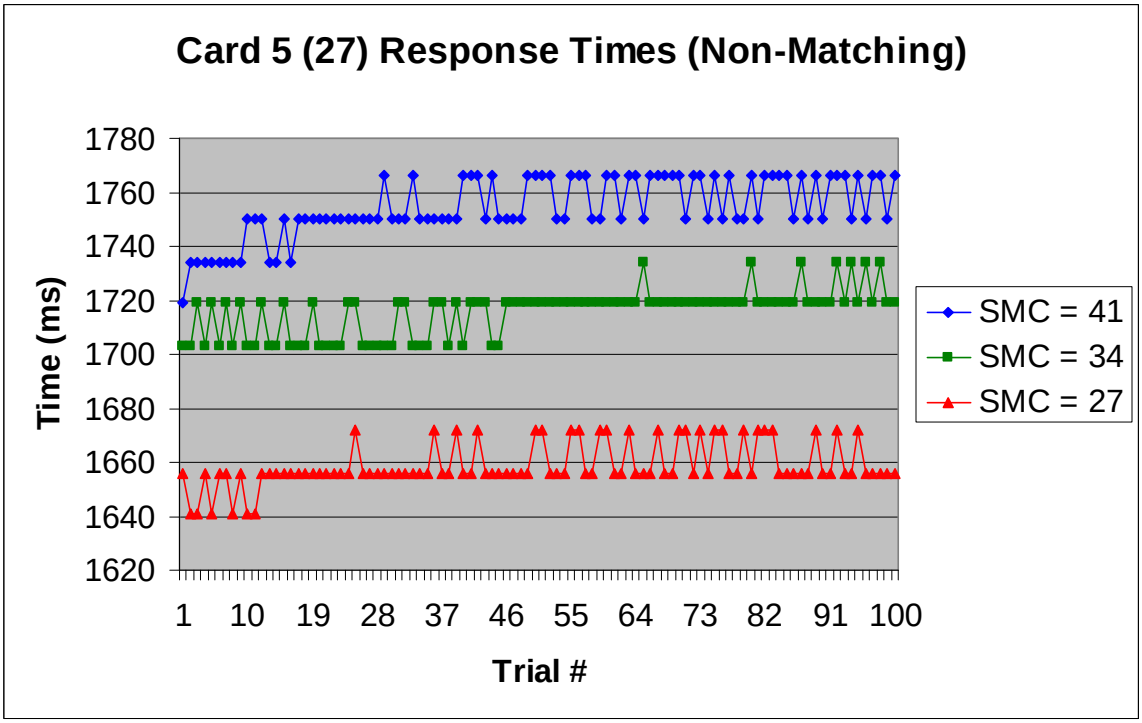


Figure C-22. Card 5 (27) Response Times for Non-Matching Templates

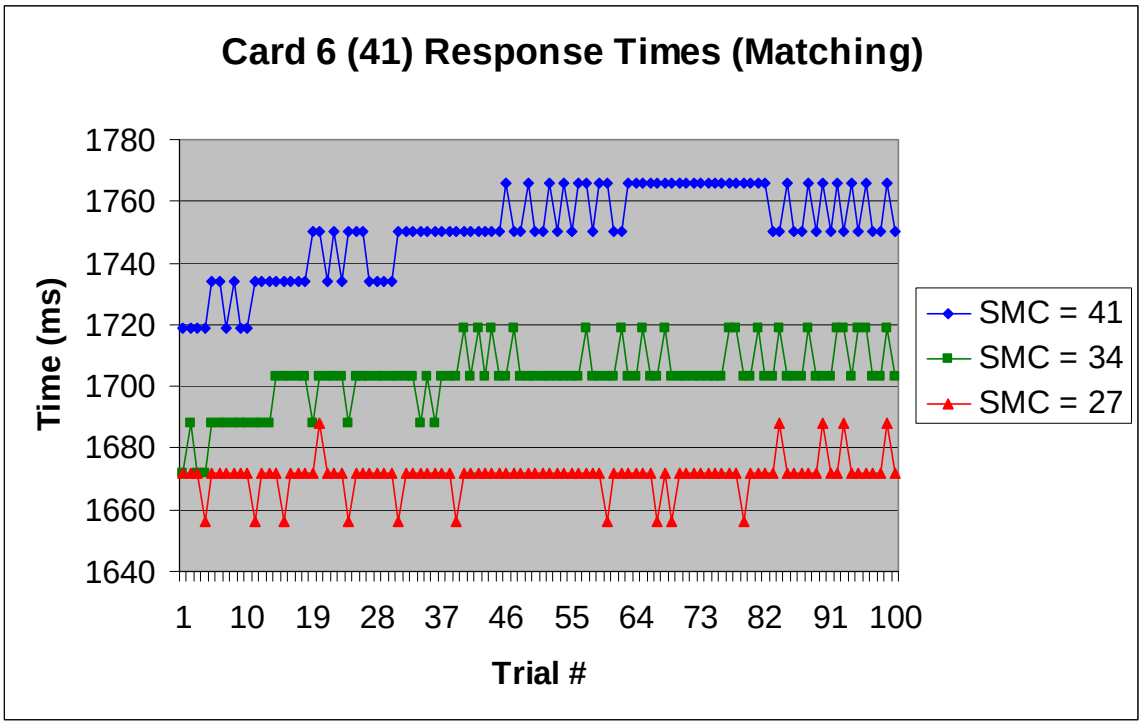


Figure C-23. Card 6 (41) Response Times for Matching Templates

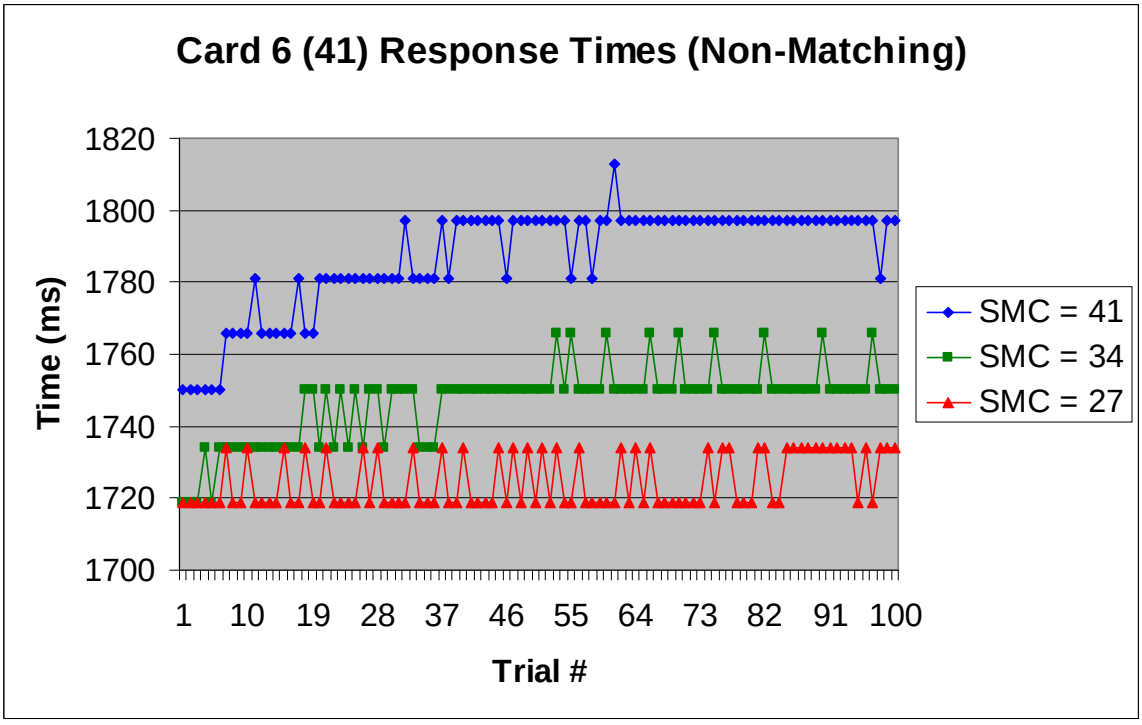


Figure C-24. Card 6 (41) Response Times for Non-Matching Templates

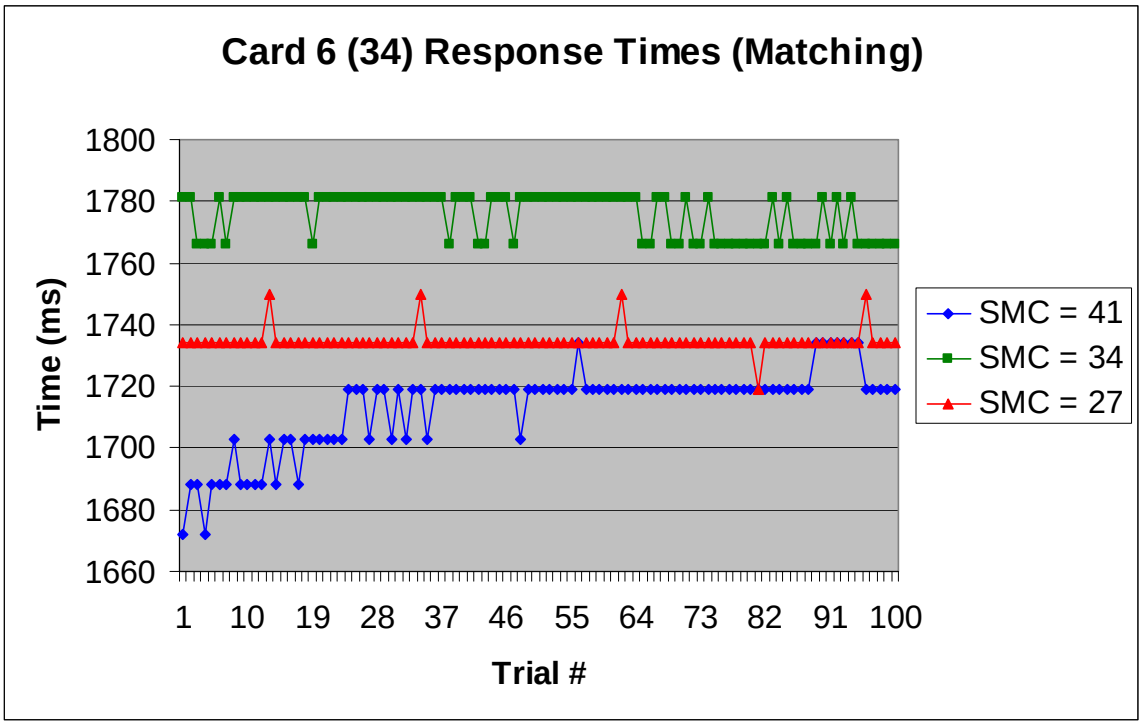


Figure C-25. Card 6 (34) Response Times for Matching Templates

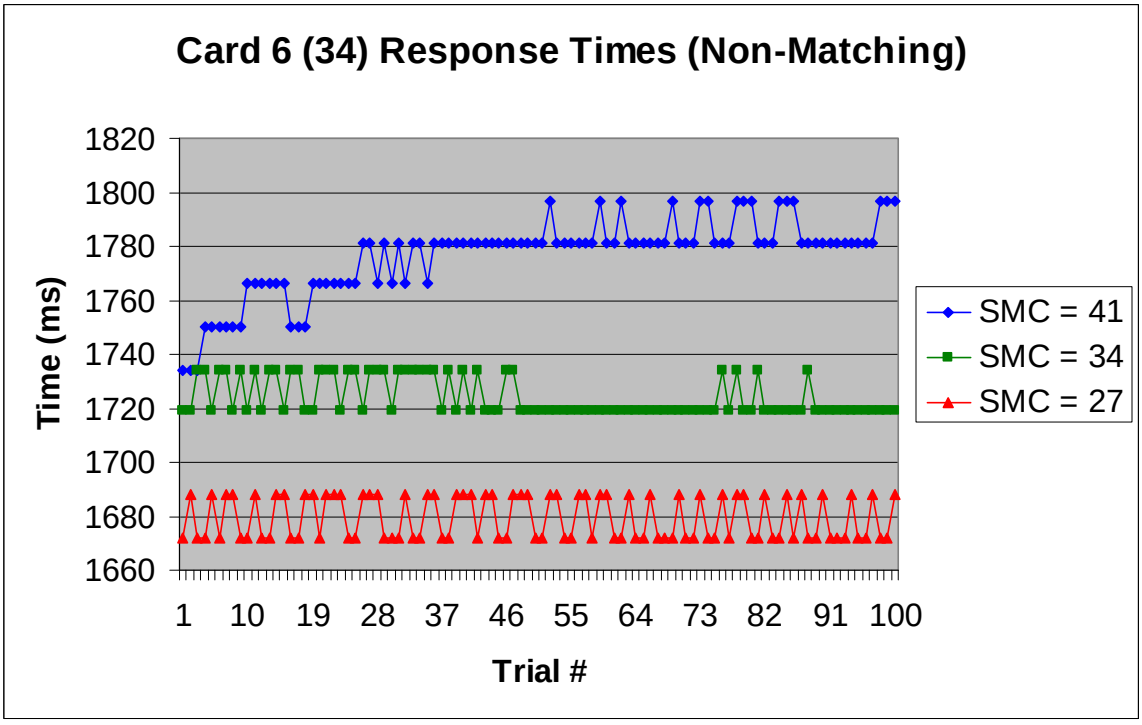


Figure C-26. Card 6 (34) Response Times for Non-Matching Templates

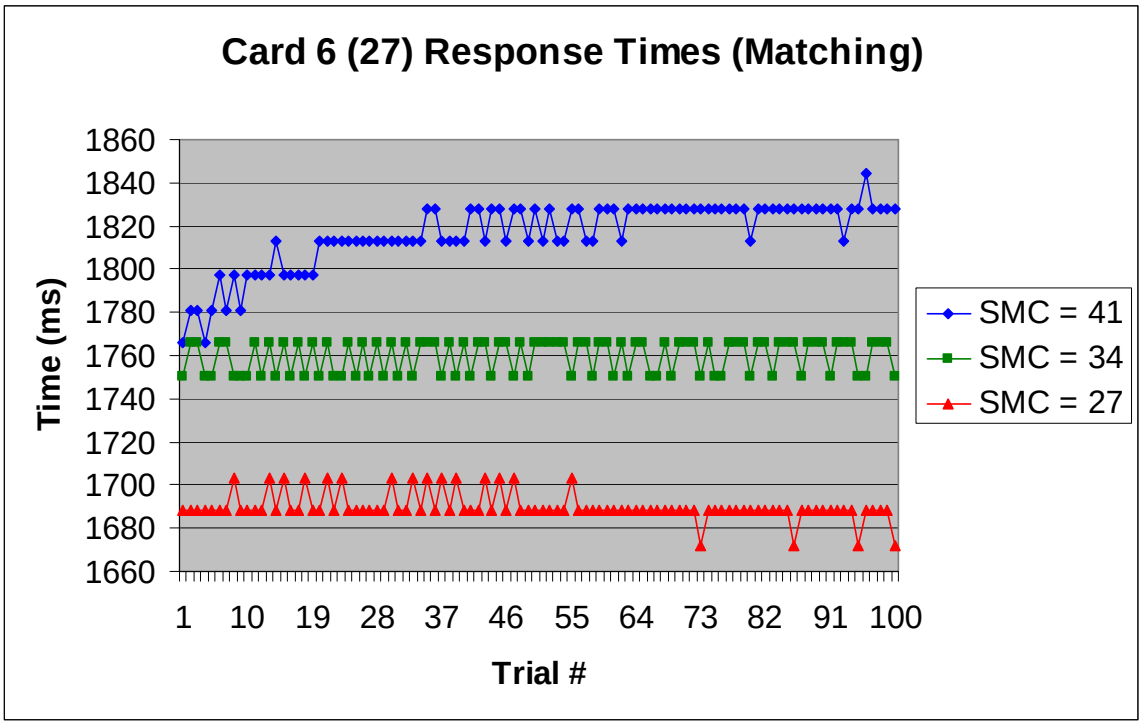


Figure C-27. Card 6 (27) Response Times for Matching Templates

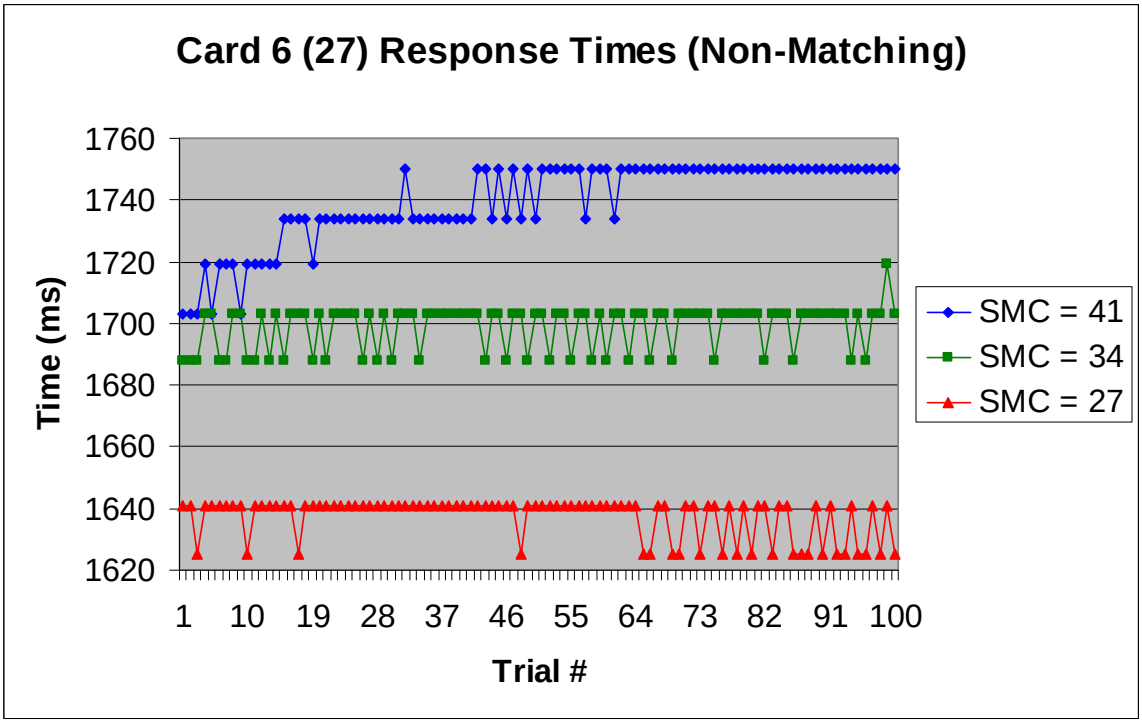


Figure C-28. Card 6 (27) Response Times for Non-Matching Templates

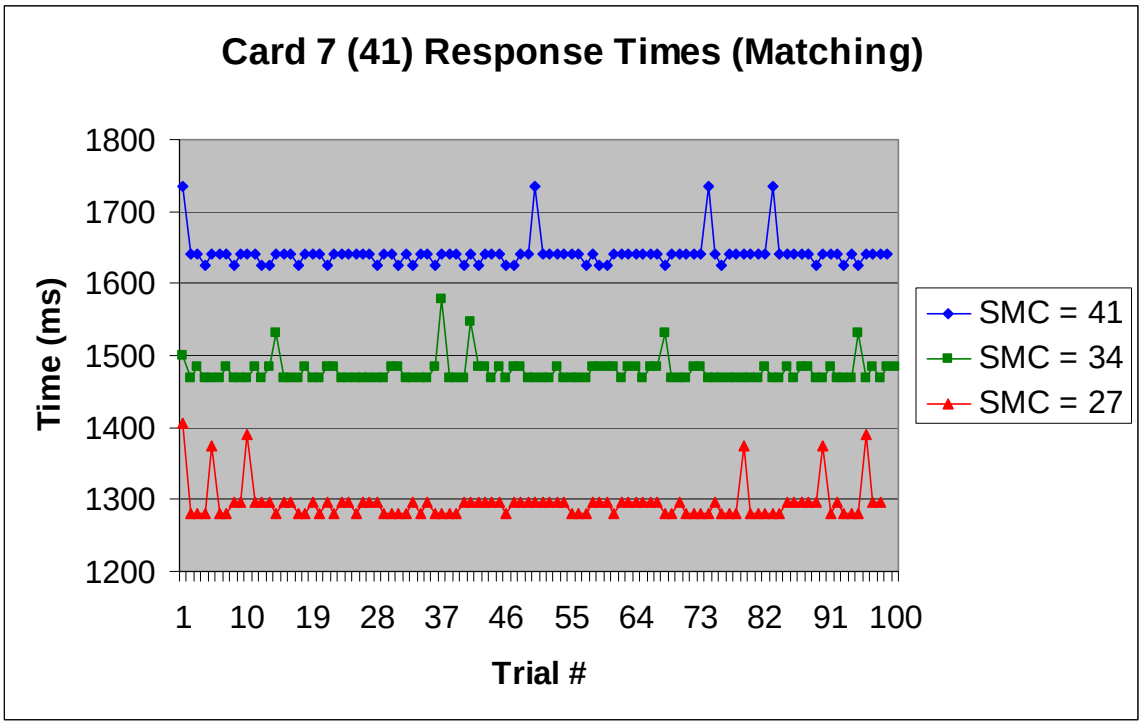


Figure C-29. Card 7 (41) Response Times for Matching Templates

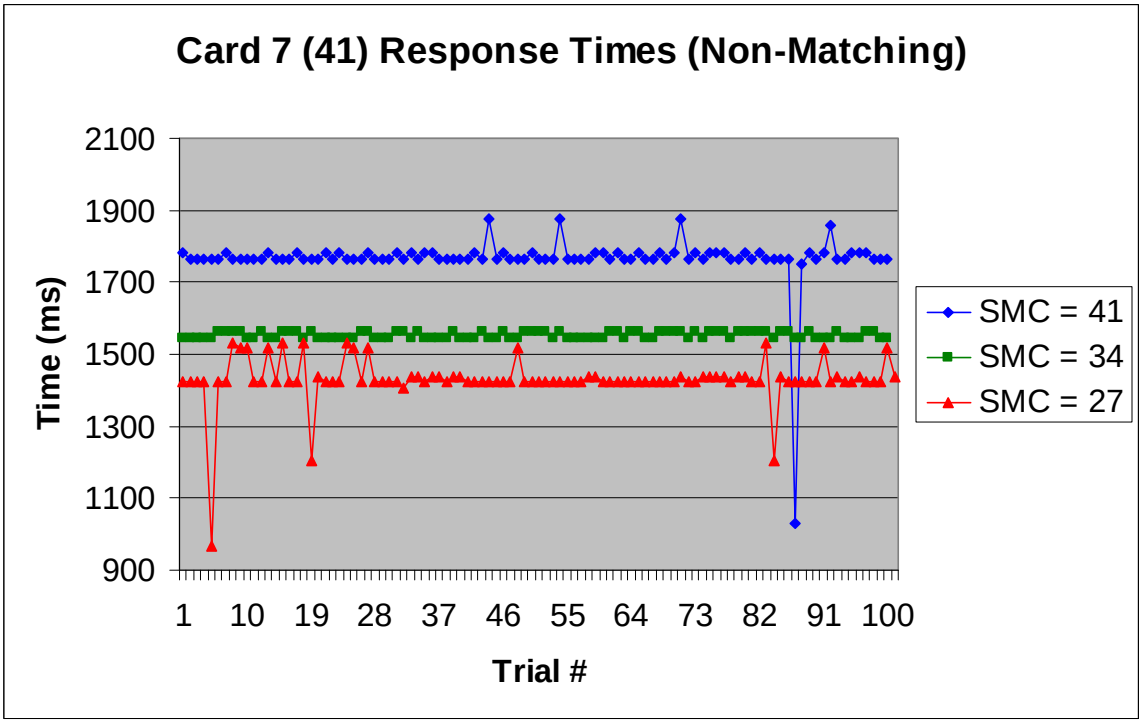


Figure C-30. Card 7 (41) Response Times for Non-Matching Templates

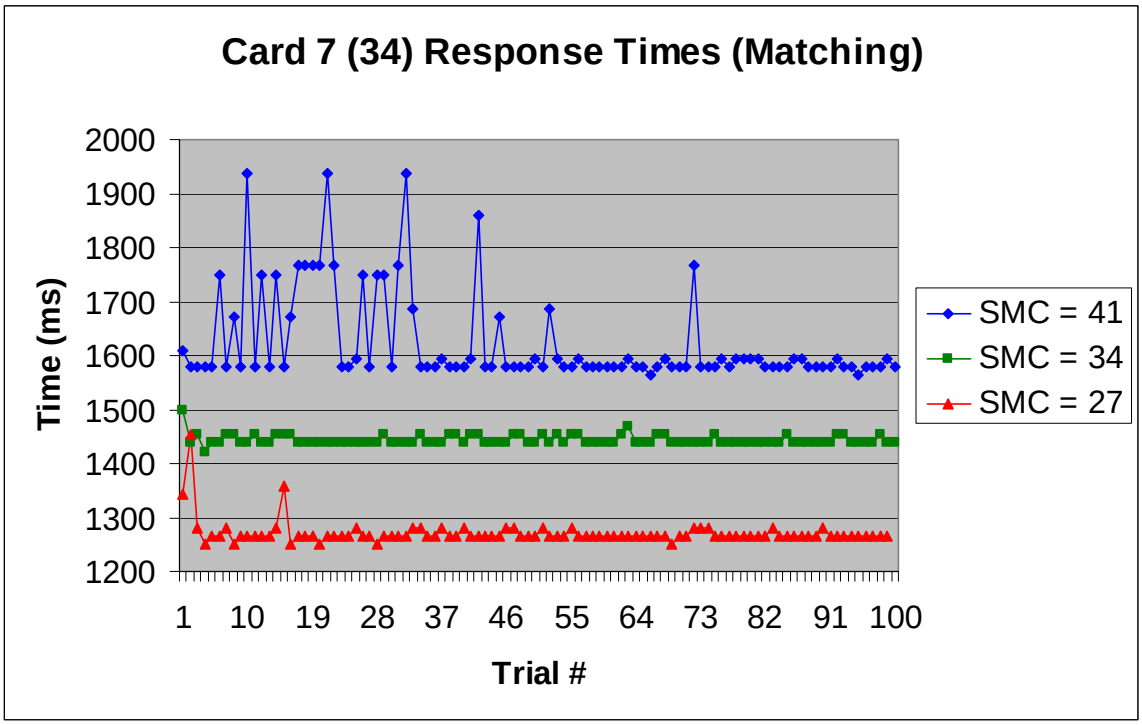


Figure C-31. Card 7 (34) Response Times for Matching Templates

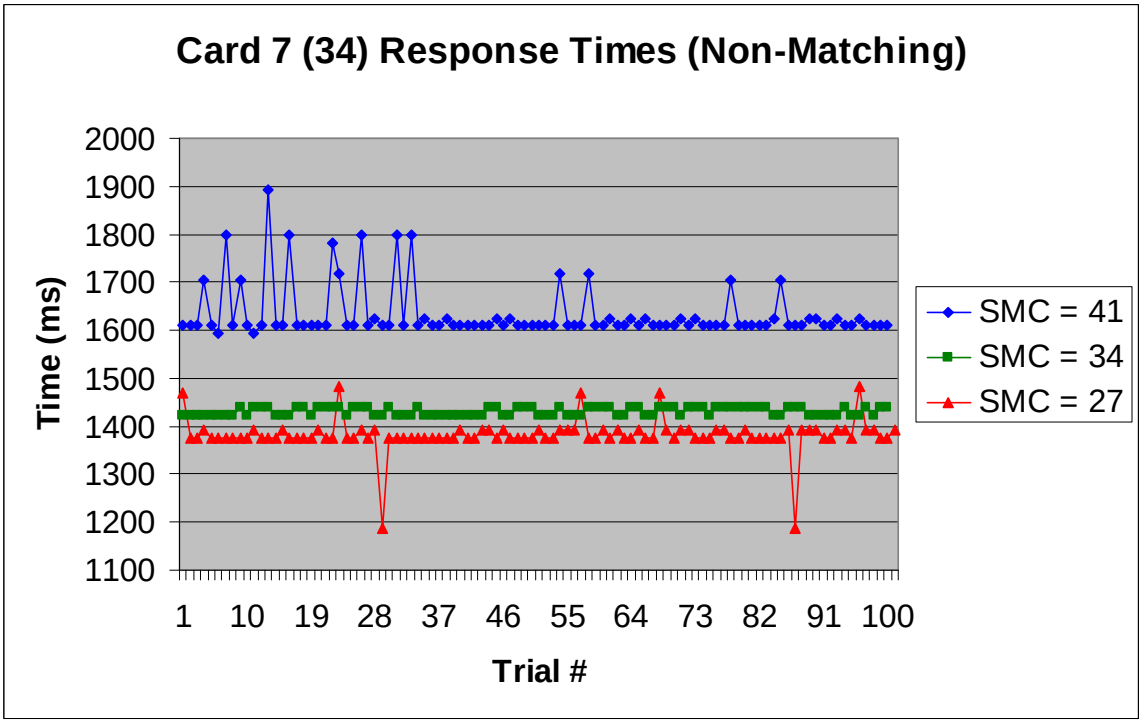


Figure C-32. Card 7 (34) Response Times for Non-Matching Templates

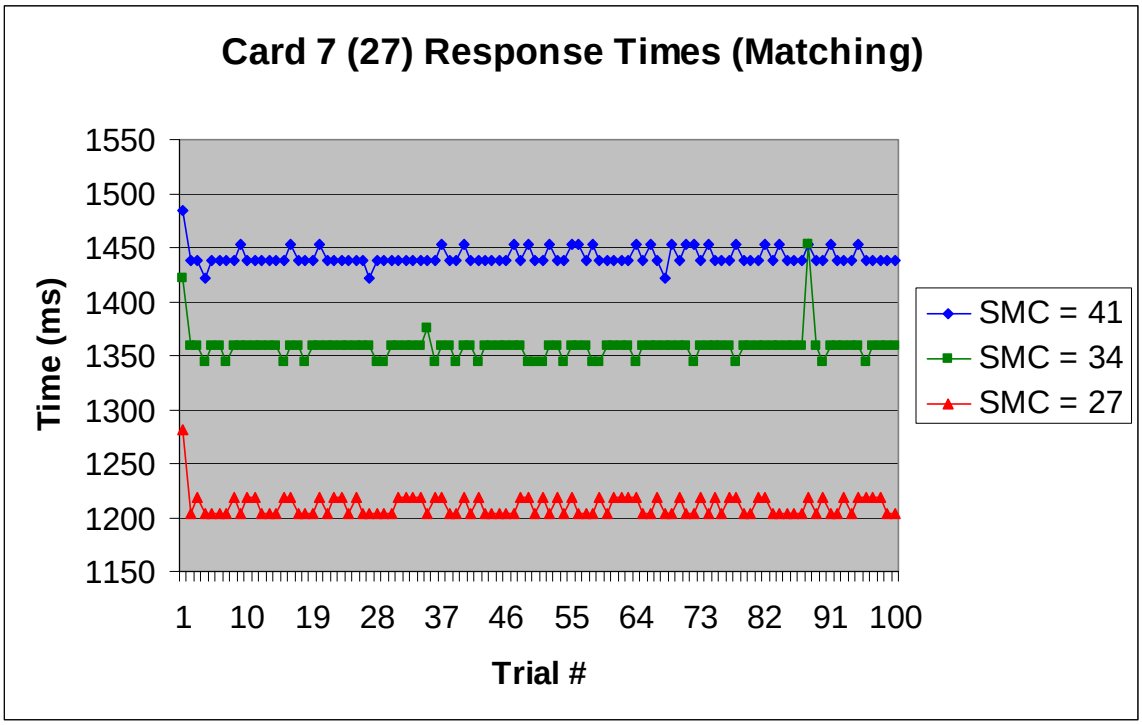


Figure C-33. Card 7 (27) Response Times for Matching Templates

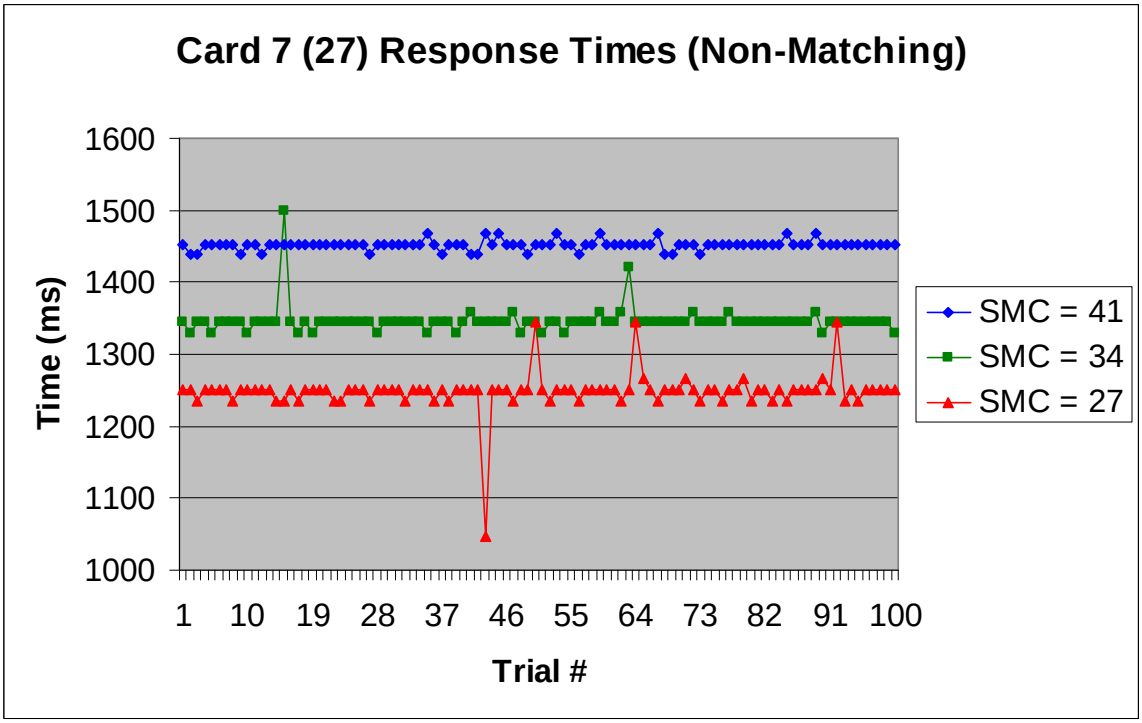


Figure C-34. Card 7 (27) Response Times for Non-Matching Templates

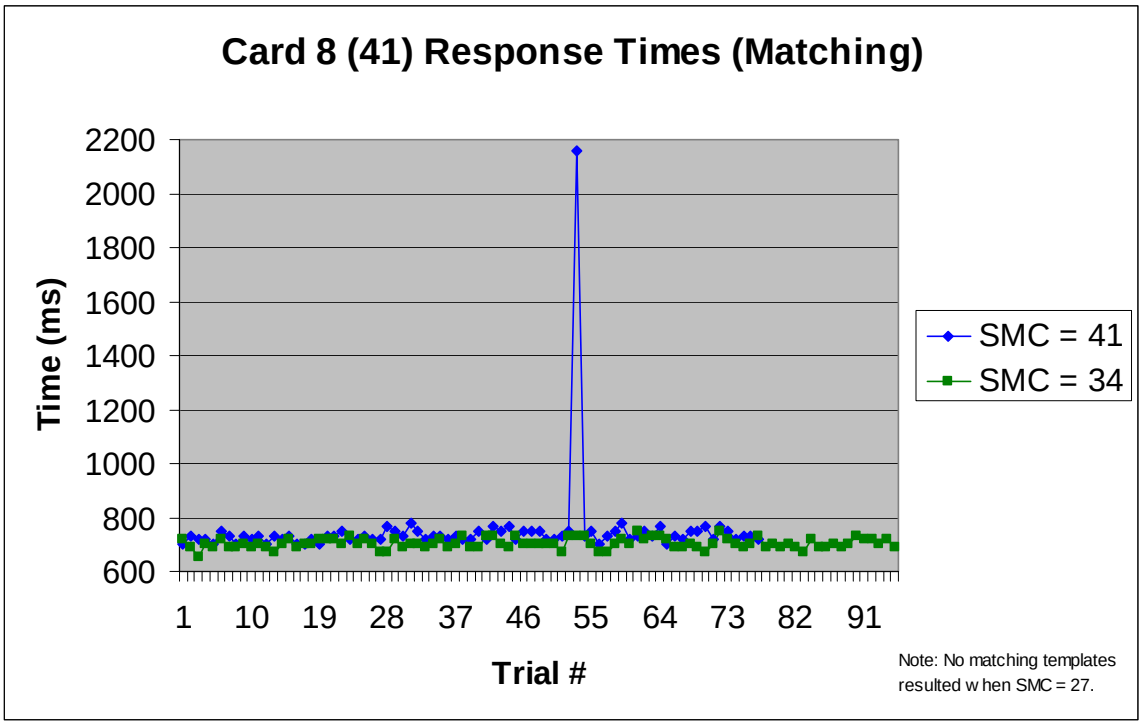


Figure C-35. Card 8 (41) Response Times for Matching Templates

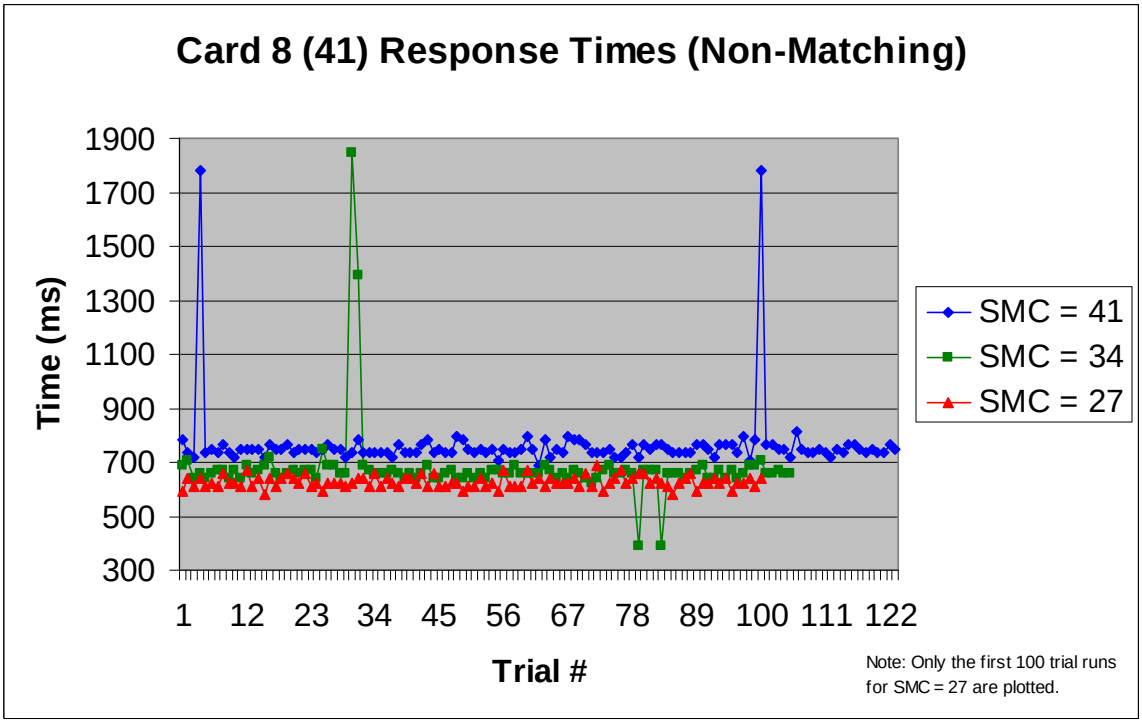


Figure C-36. Card 8 (41) Response Times for Non-Matching Templates

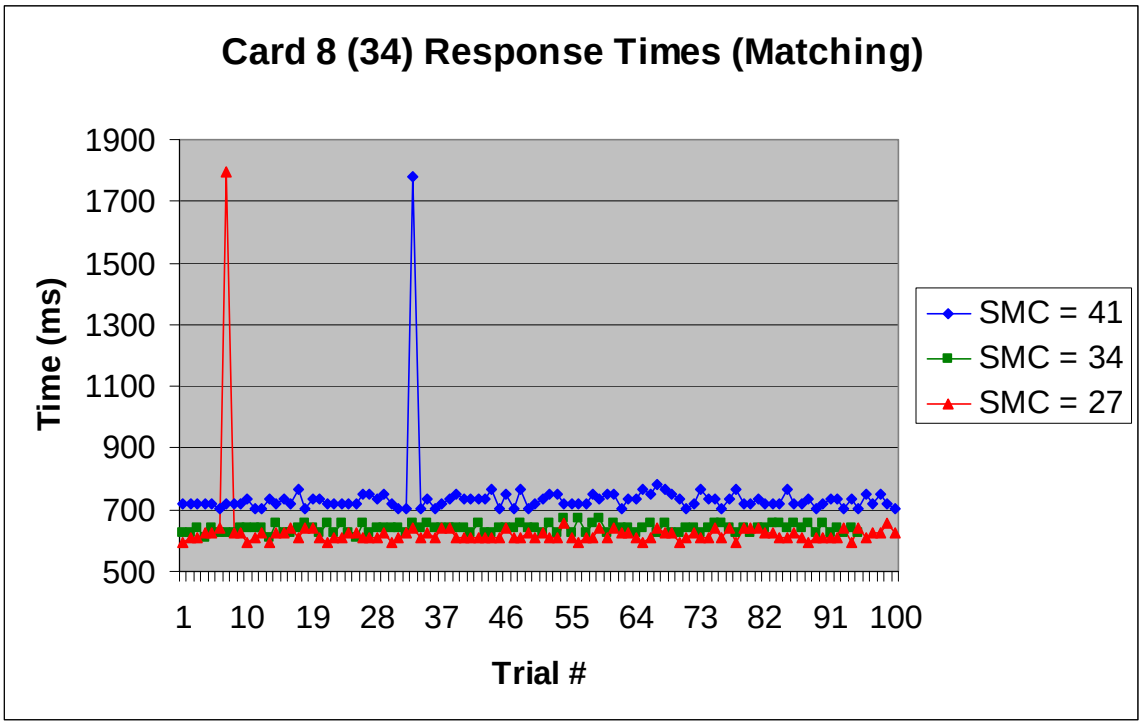


Figure C-37. Card 8 (34) Response Times for Matching Templates

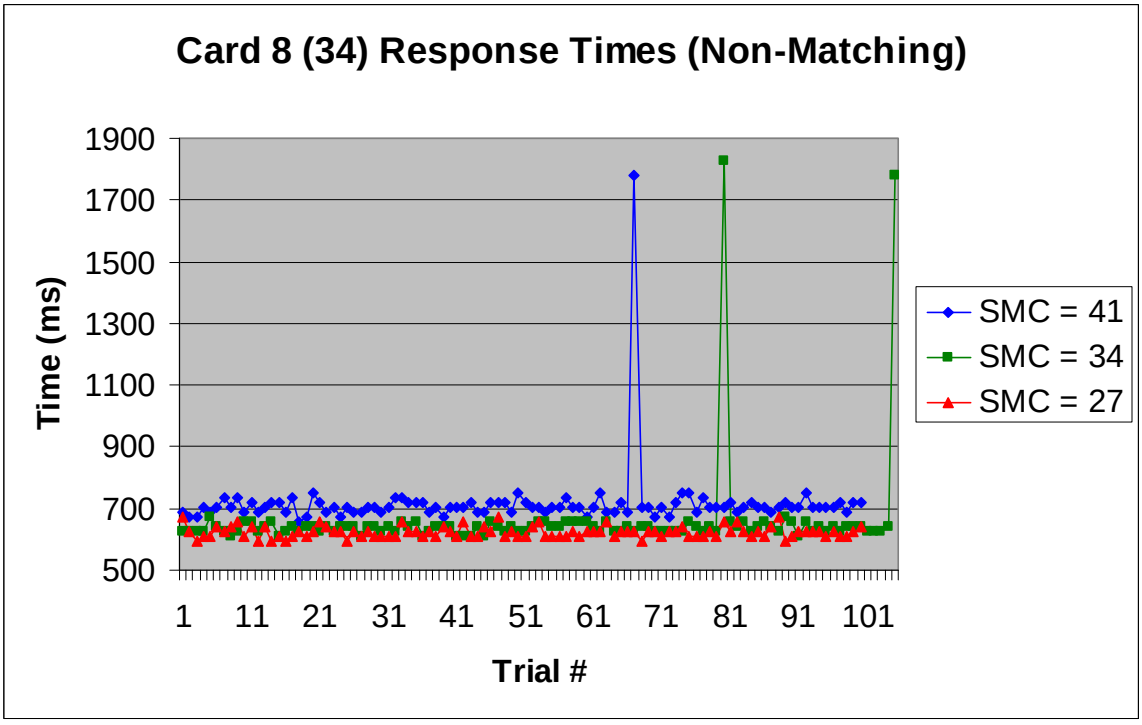


Figure C-38. Card 8 (34) Response Times for Non-Matching Templates

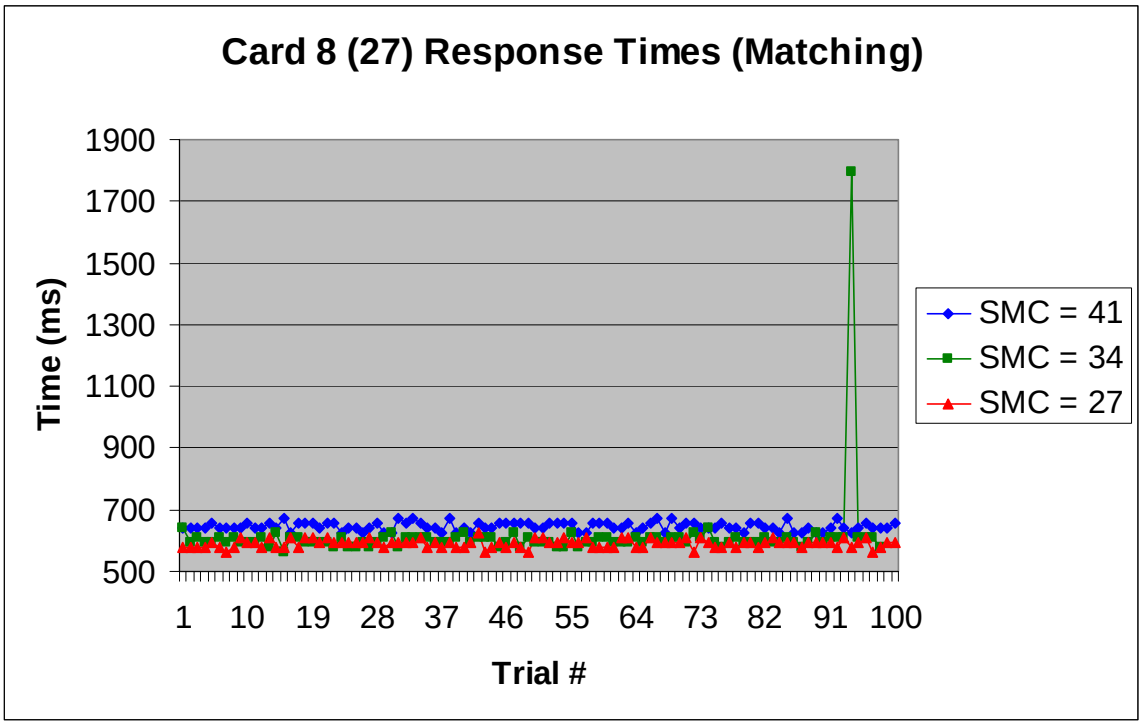


Figure C-39. Card 8 (27) Response Times for Matching Templates

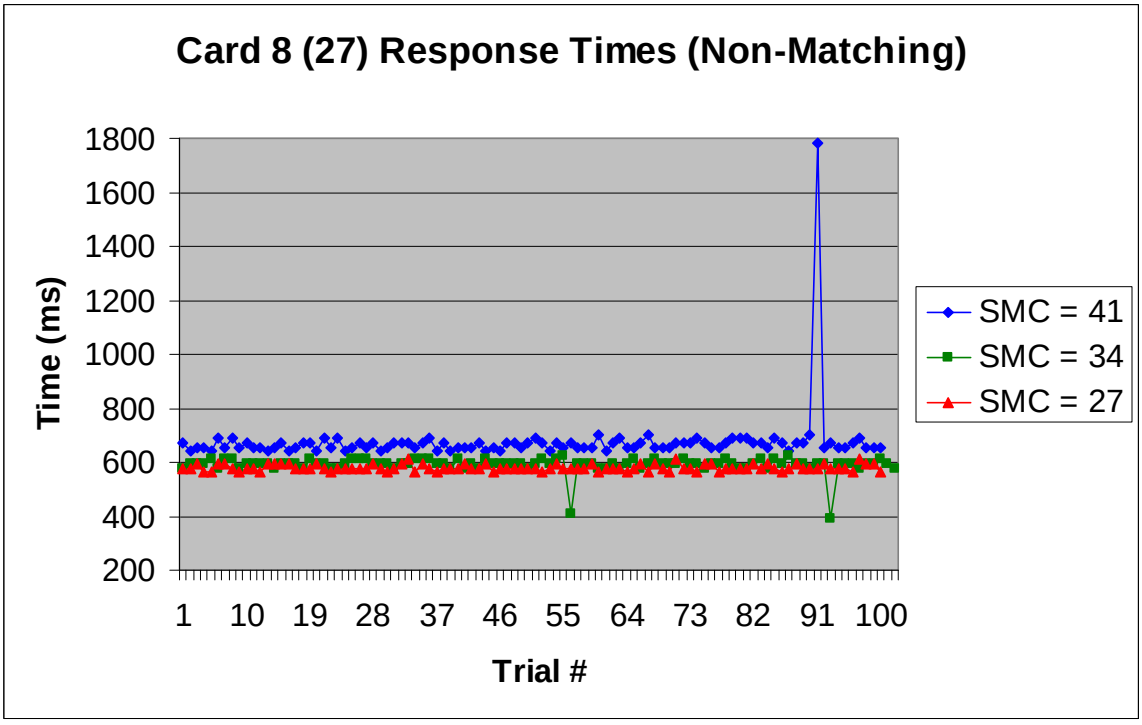


Figure C-40. Card 8 (27) Response Times for Non-Matching Templates

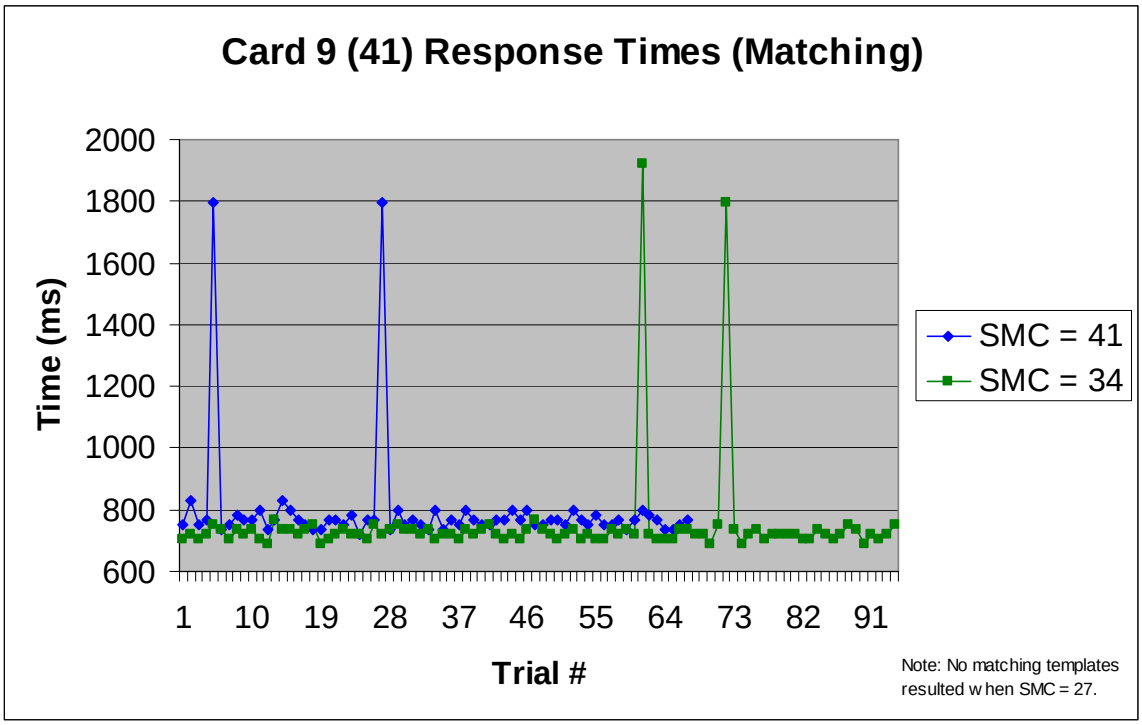


Figure C-41. Card 9 (41) Response Times for Matching Templates

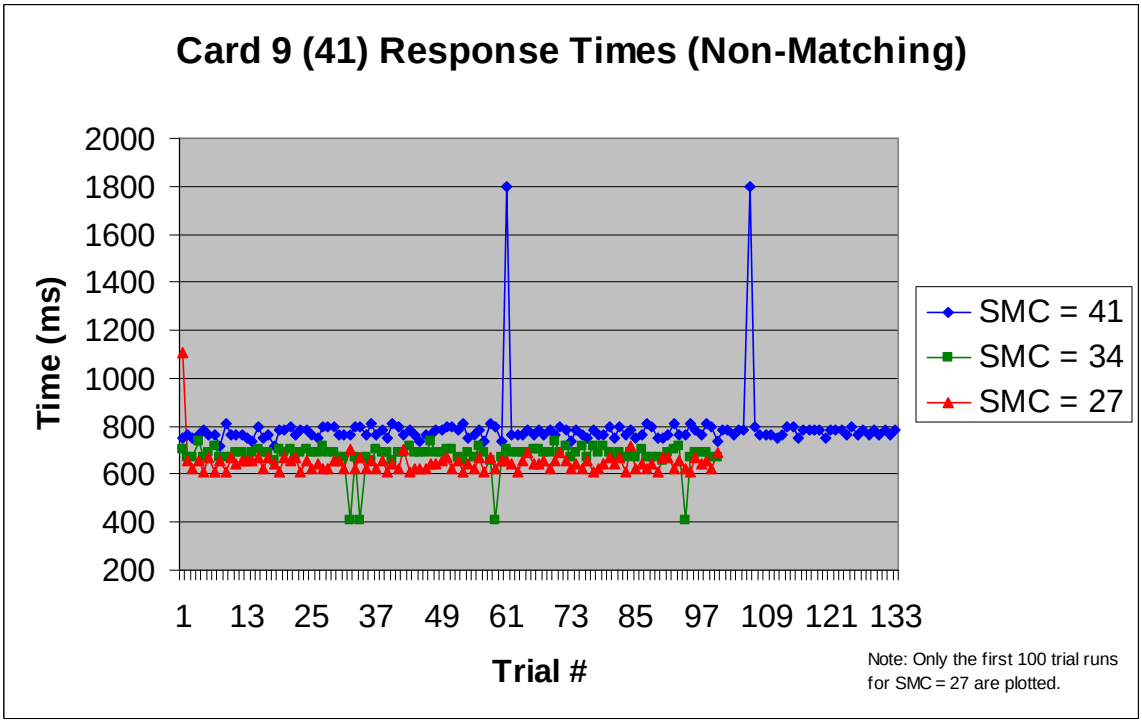


Figure C-42. Card 9 (41) Response Times for Non-Matching Templates

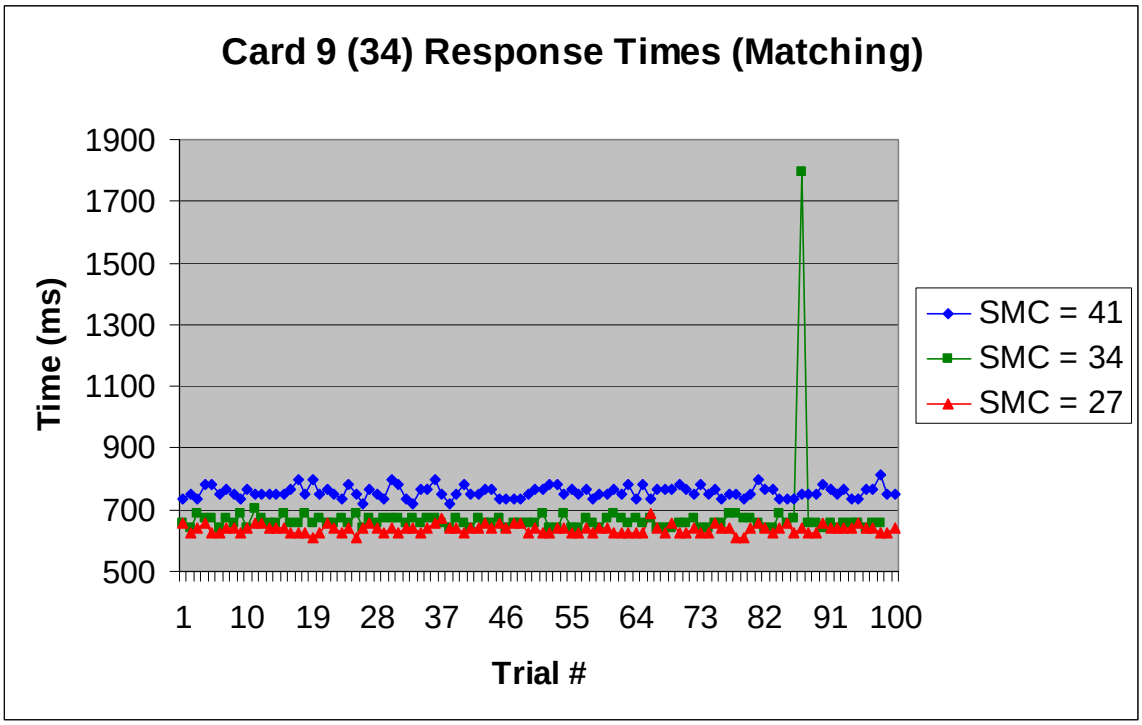


Figure C-43. Card 9 (34) Response Times for Matching Templates

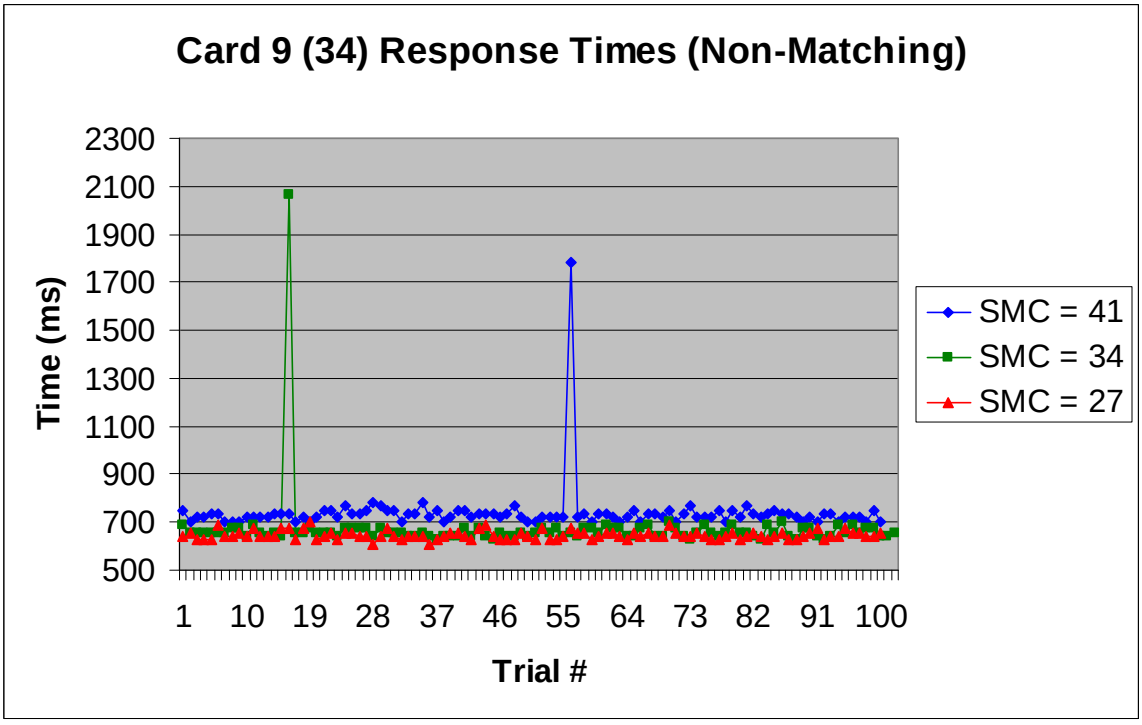


Figure C-44. Card 9 (34) Response Times for Non-Matching Templates

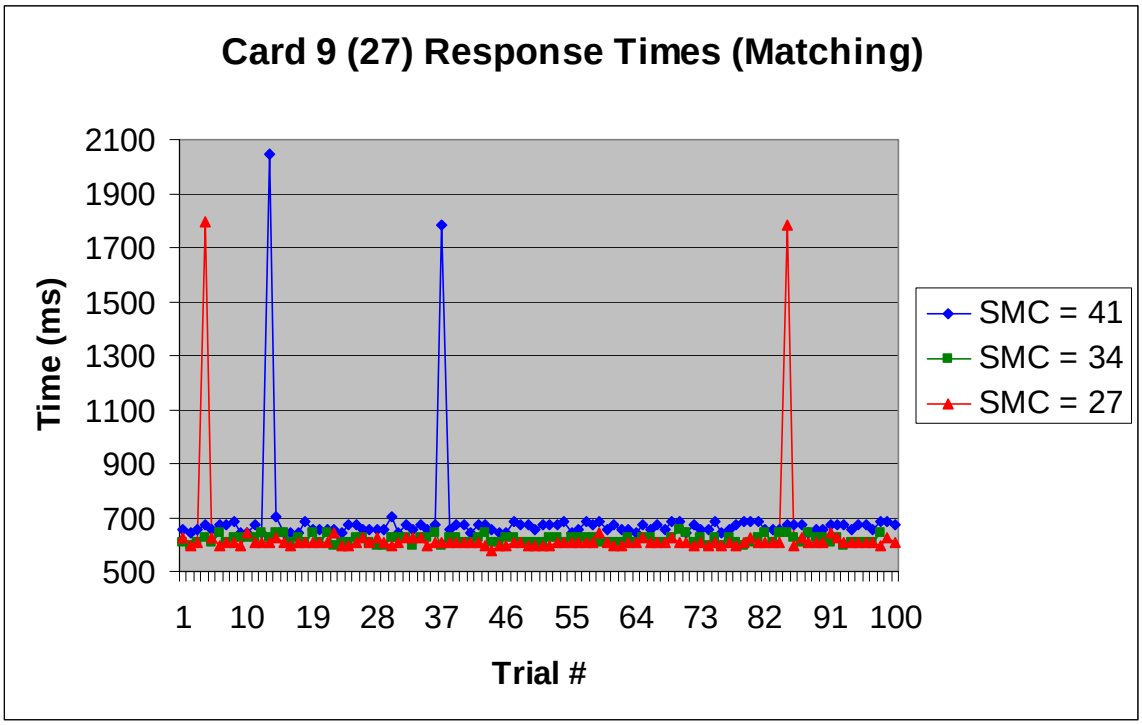


Figure C-45. Card 9 (27) Response Times for Matching Templates

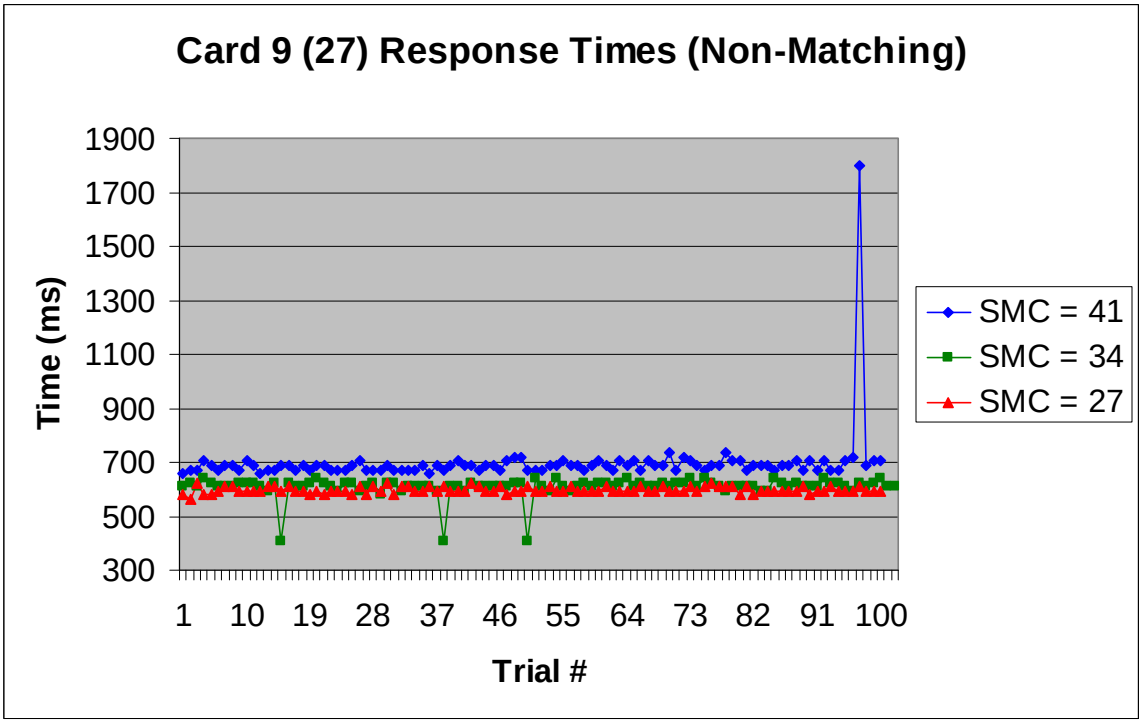


Figure C-46. Card 9 (27) Response Times for Non-Matching Templates

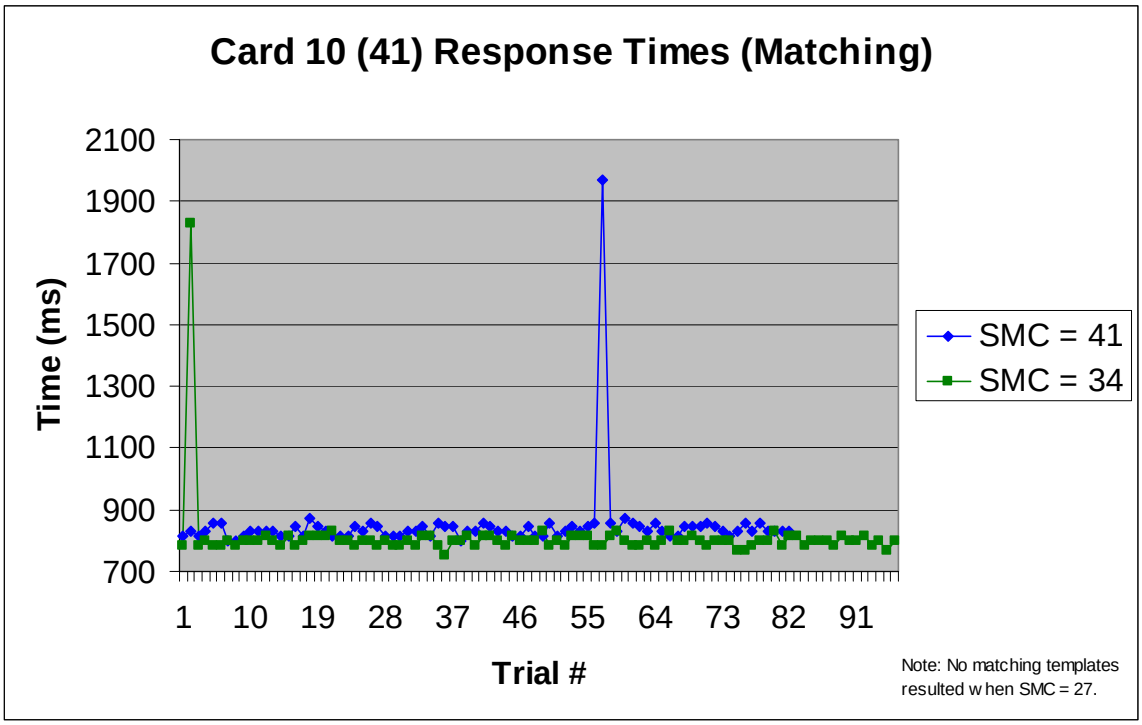


Figure C-47. Card 10 (41) Response Times for Matching Templates

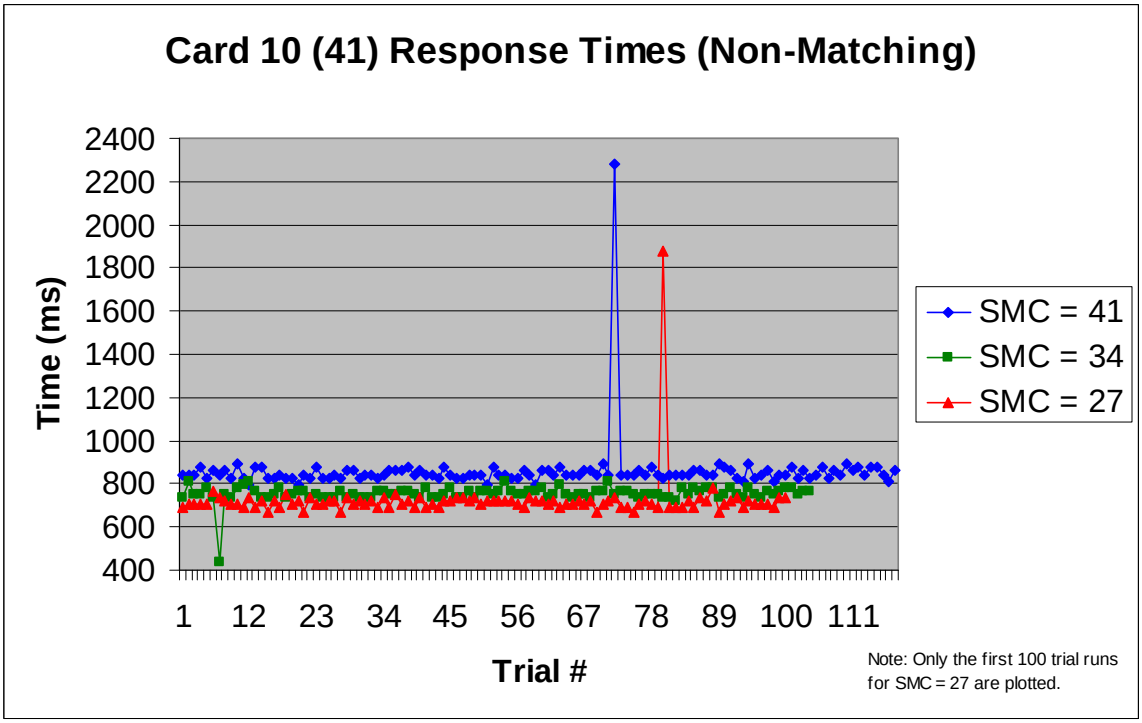


Figure C-48. Card 10 (41) Response Times for Non-Matching Templates

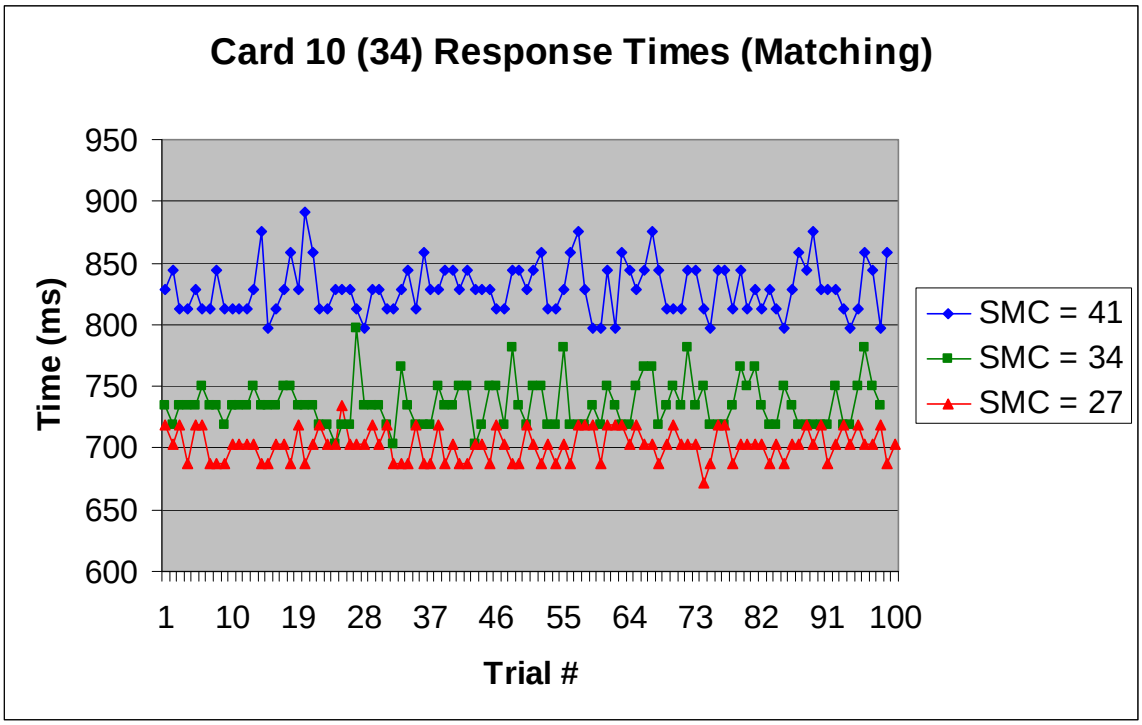


Figure C-49. Card 10 (34) Response Times for Matching Templates

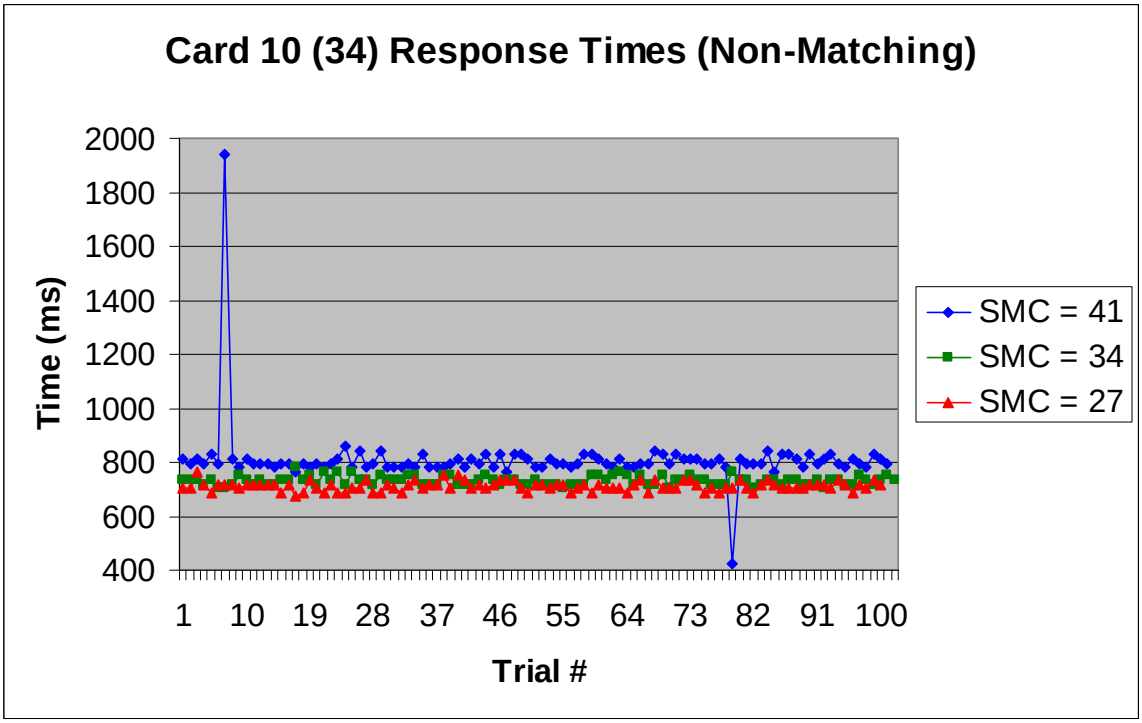


Figure C-50. Card 10 (34) Response Times for Non-Matching Templates

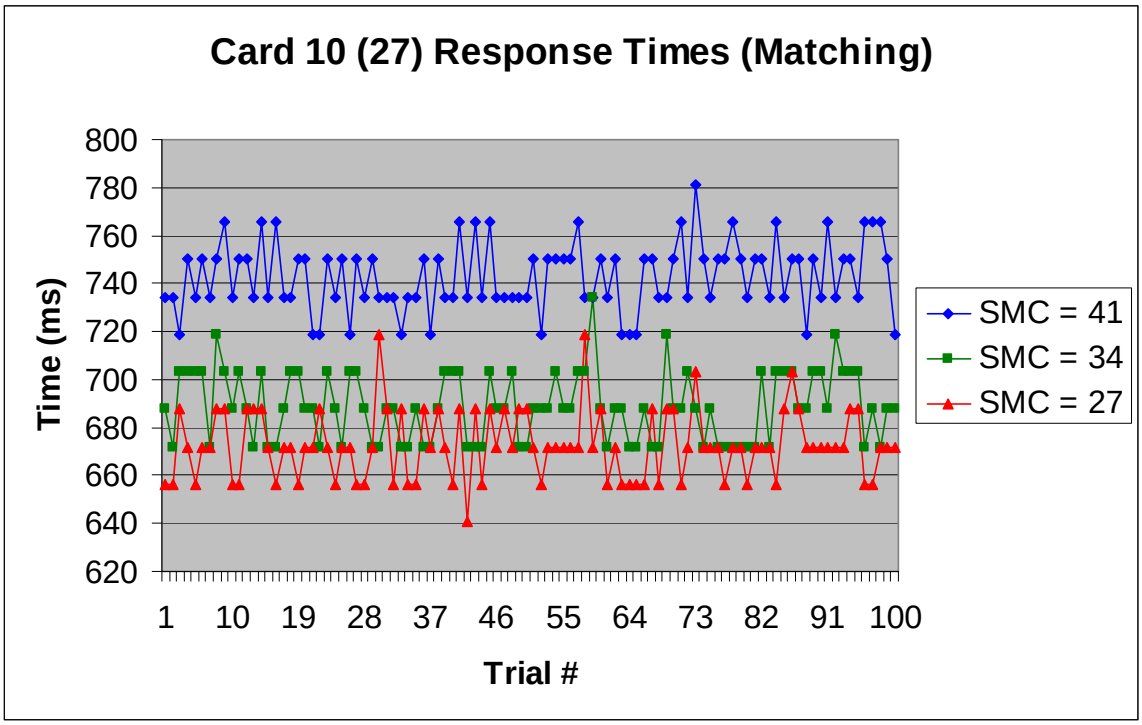


Figure C-51. Card 10 (27) Response Times for Matching Templates

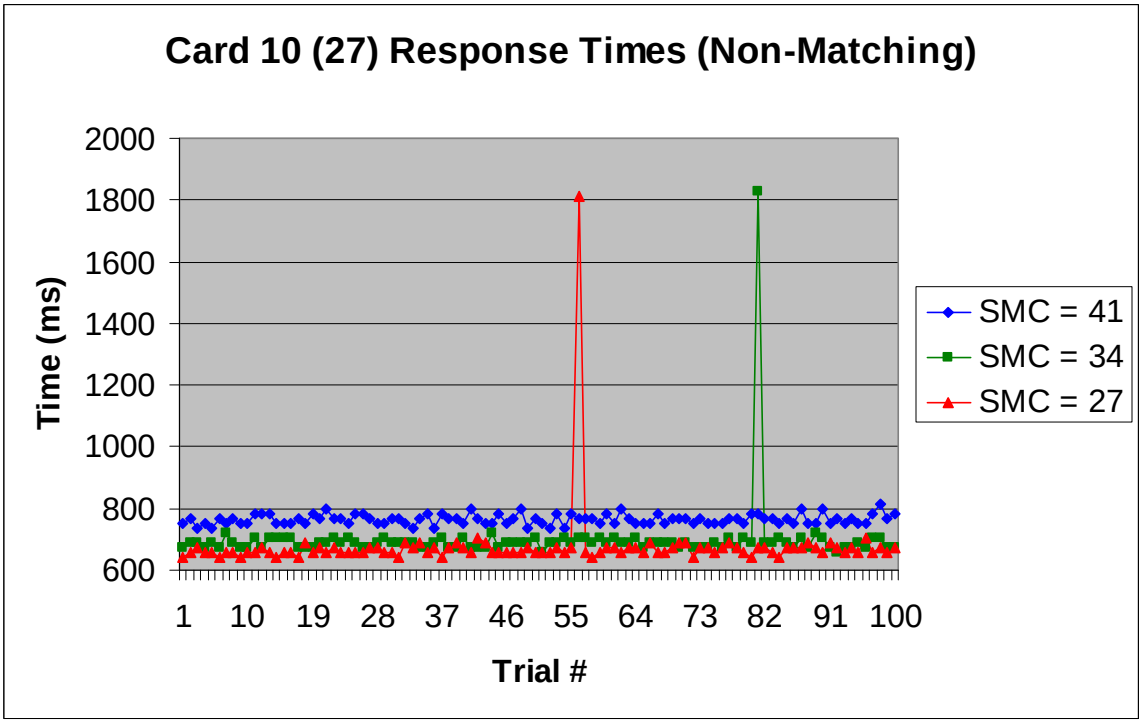


Figure C-52. Card 10 (27) Response Times for Non-Matching Templates

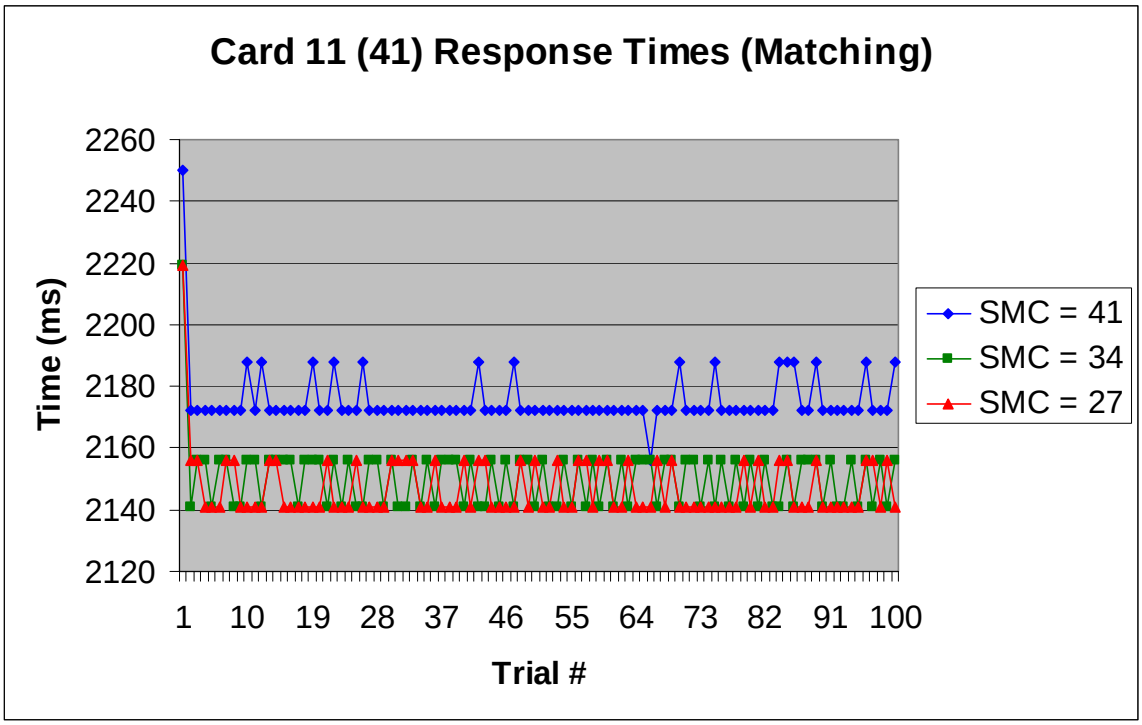


Figure C-53. Card 11 (41) Response Times for Matching Templates

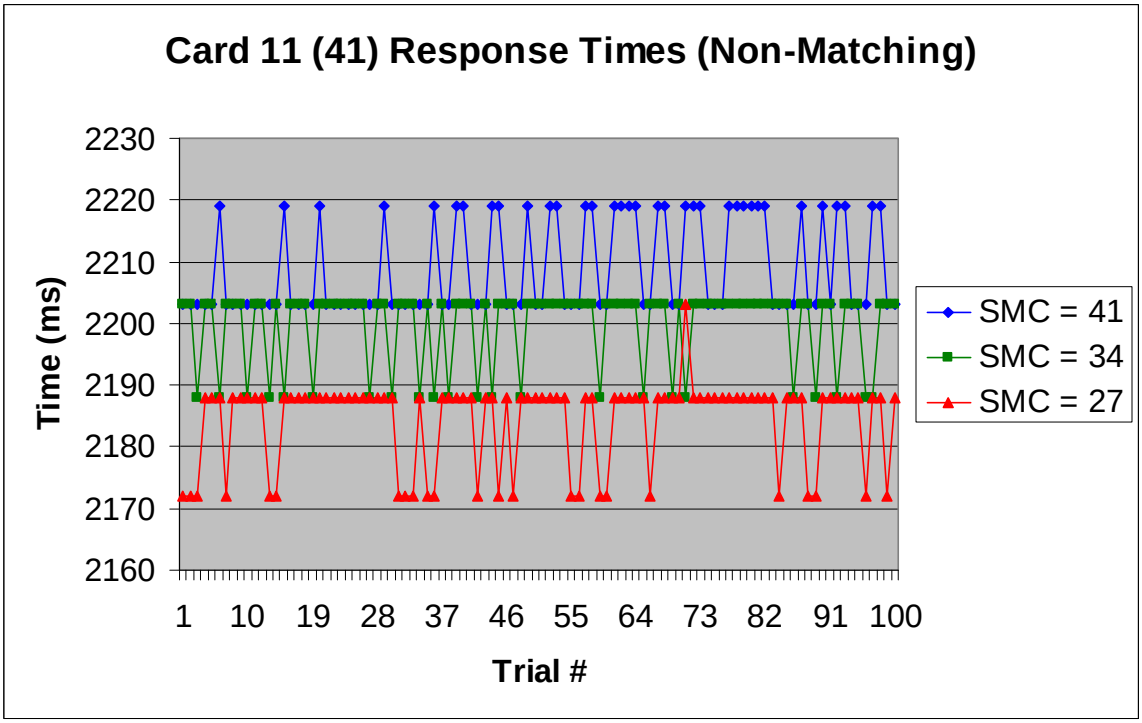


Figure C-54. Card 11 (41) Response Times for Non-Matching Templates

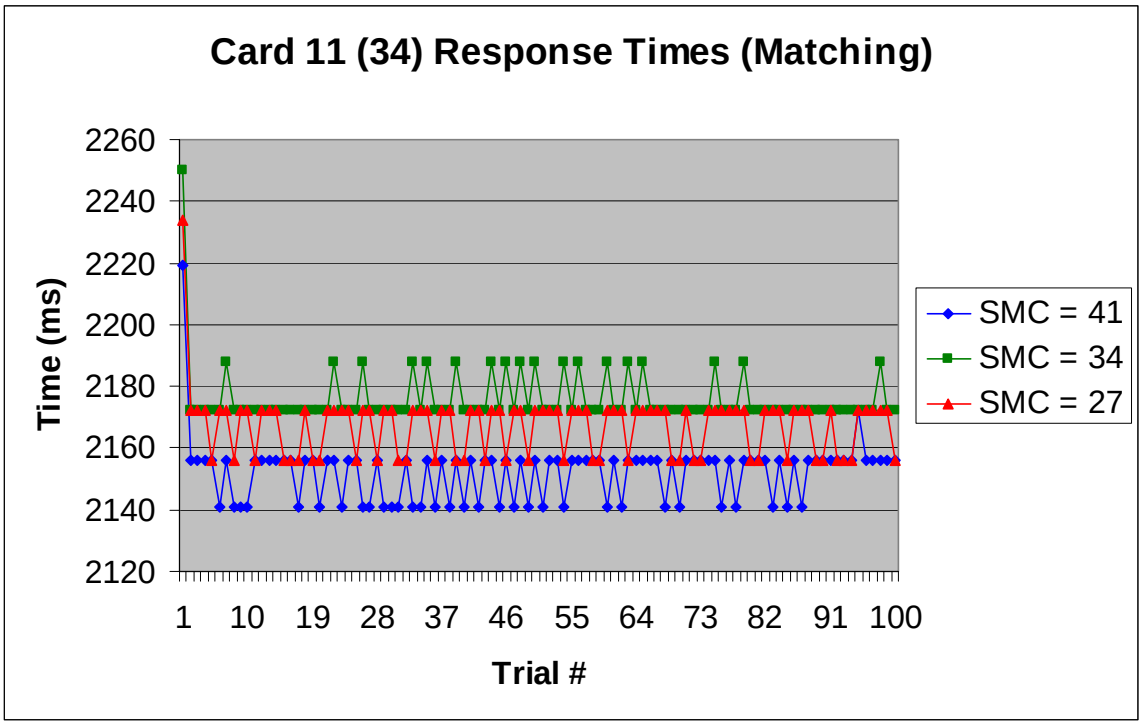


Figure C-55. Card 11 (34) Response Times for Matching Templates

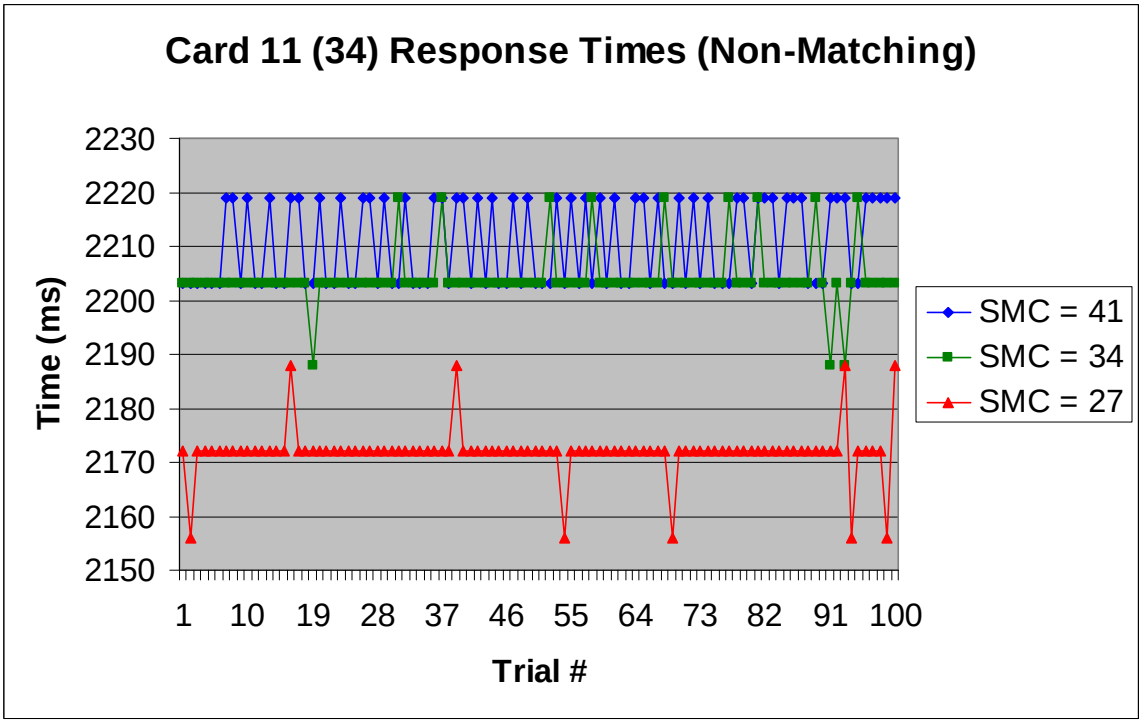


Figure C-56. Card 11 (34) Response Times for Non-Matching Templates

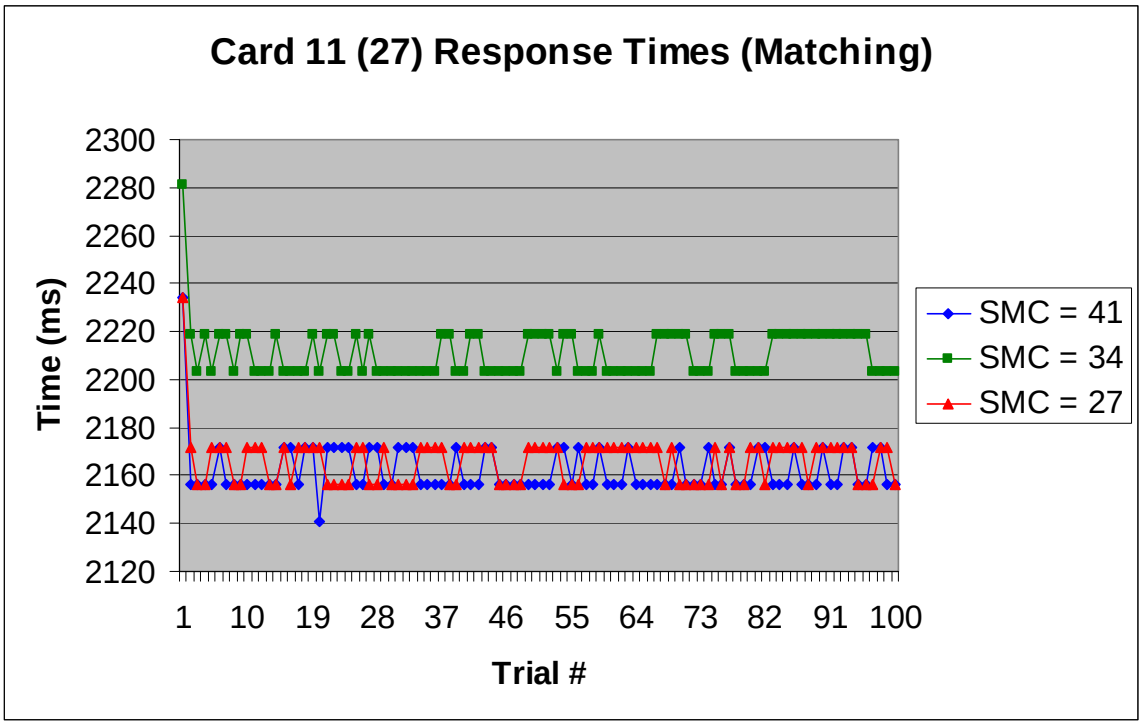


Figure C-57. Card 11 (27) Response Times for Matching Templates

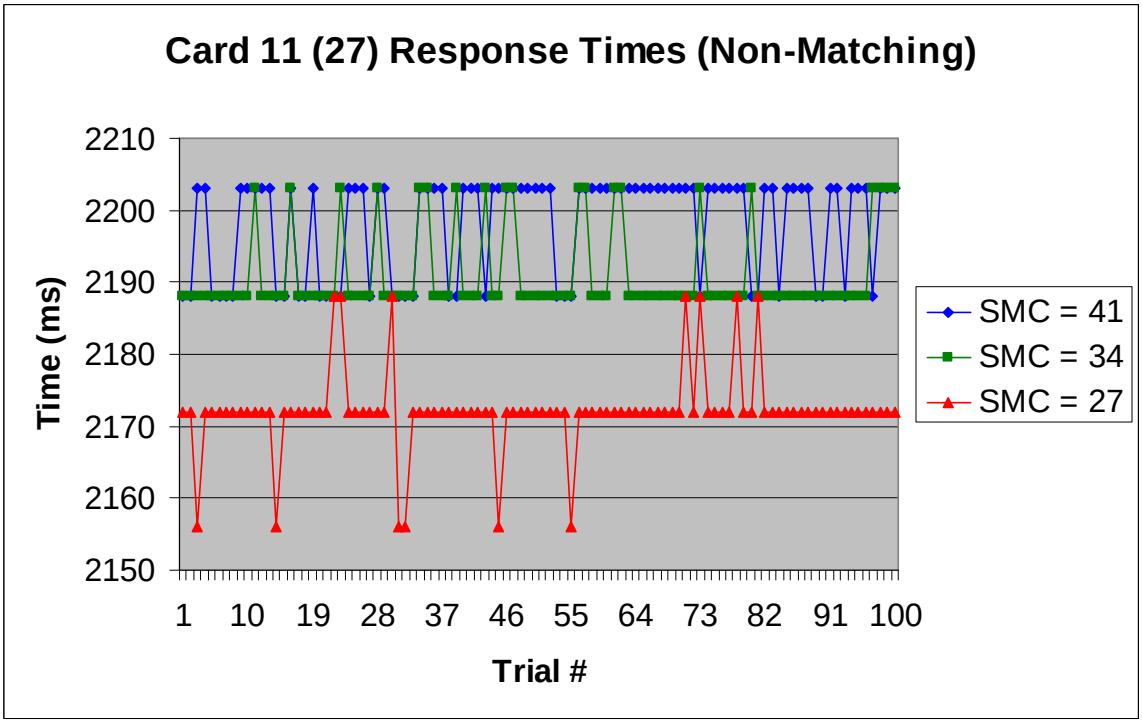


Figure C-58. Card 11 (27) Response Times for Non-Matching Templates

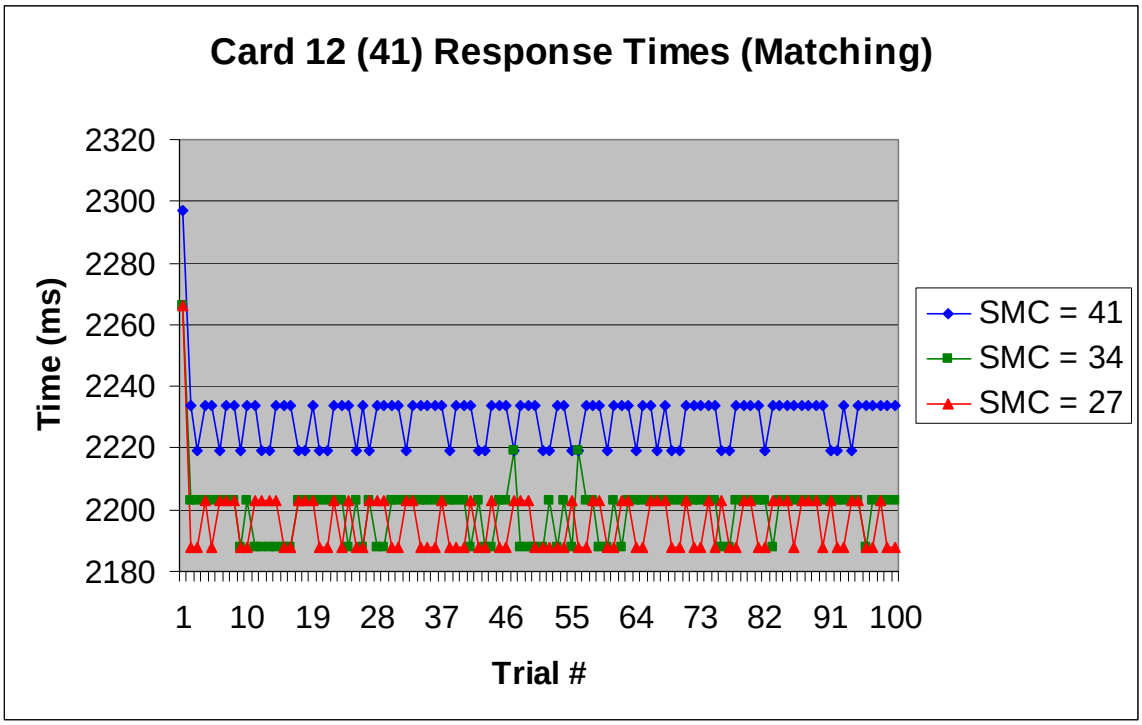


Figure C-59. Card 12 (41) Response Times for Matching Templates

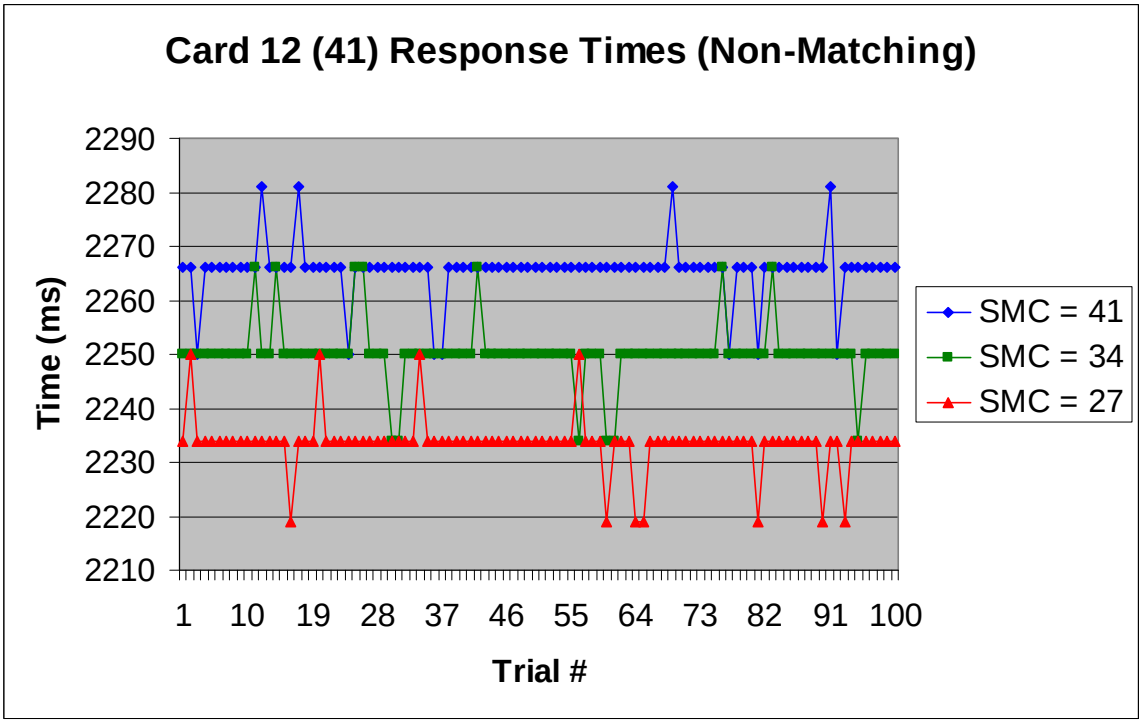


Figure C-60. Card 12 (41) Response Times for Non-Matching Templates

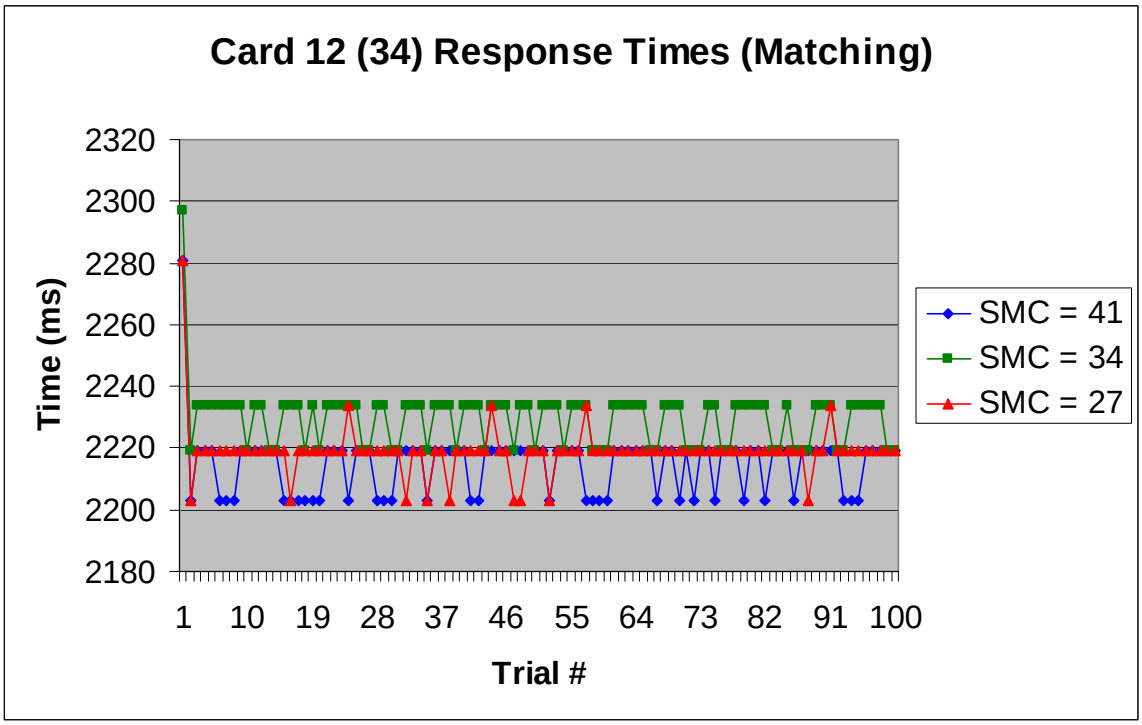


Figure C-61. Card 12 (34) Response Times for Matching Templates

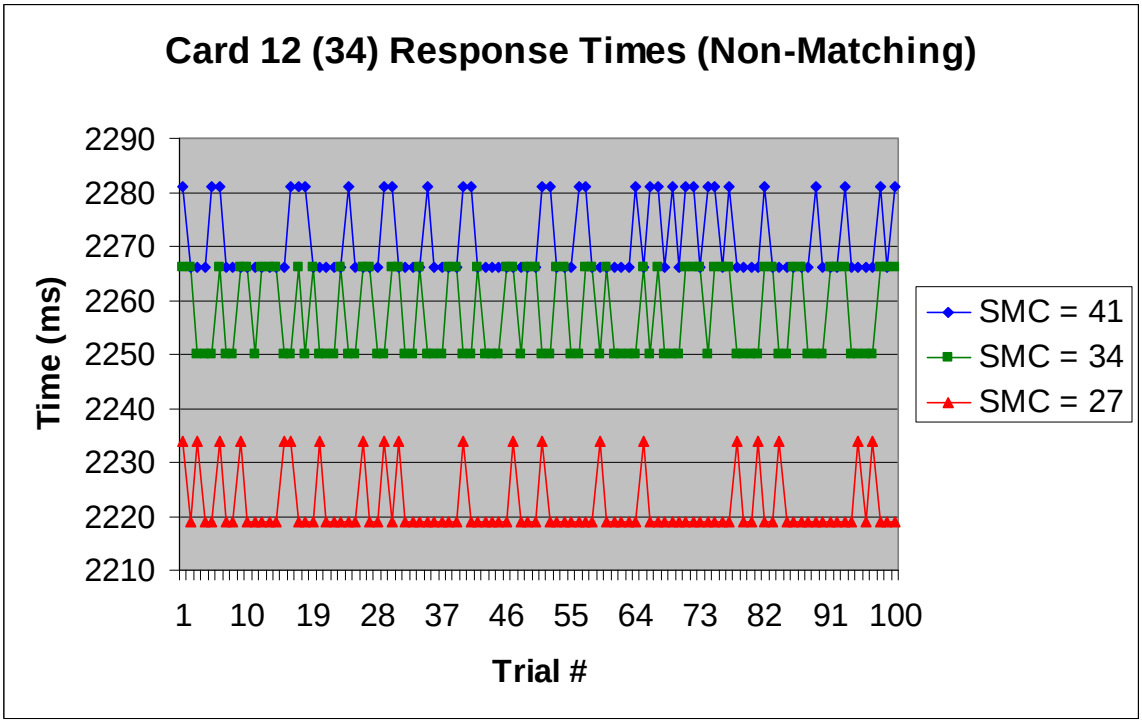


Figure C-62. Card 12 (34) Response Times for Non-Matching Templates

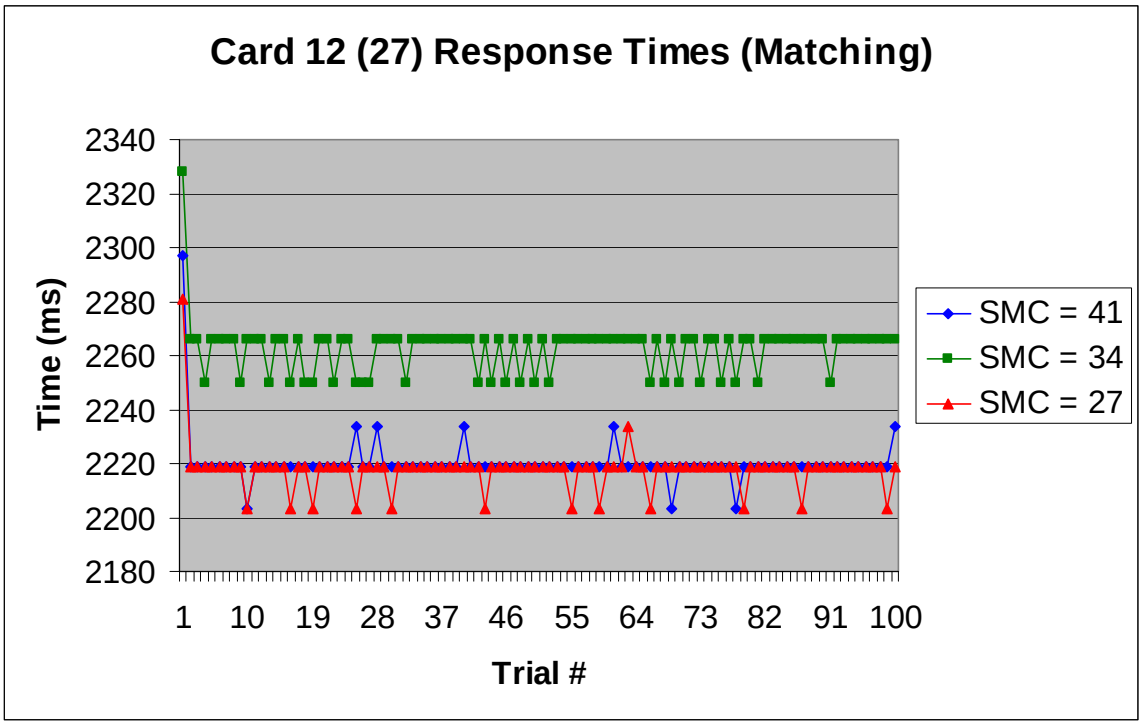


Figure C-63. Card 12 (27) Response Times for Matching Templates

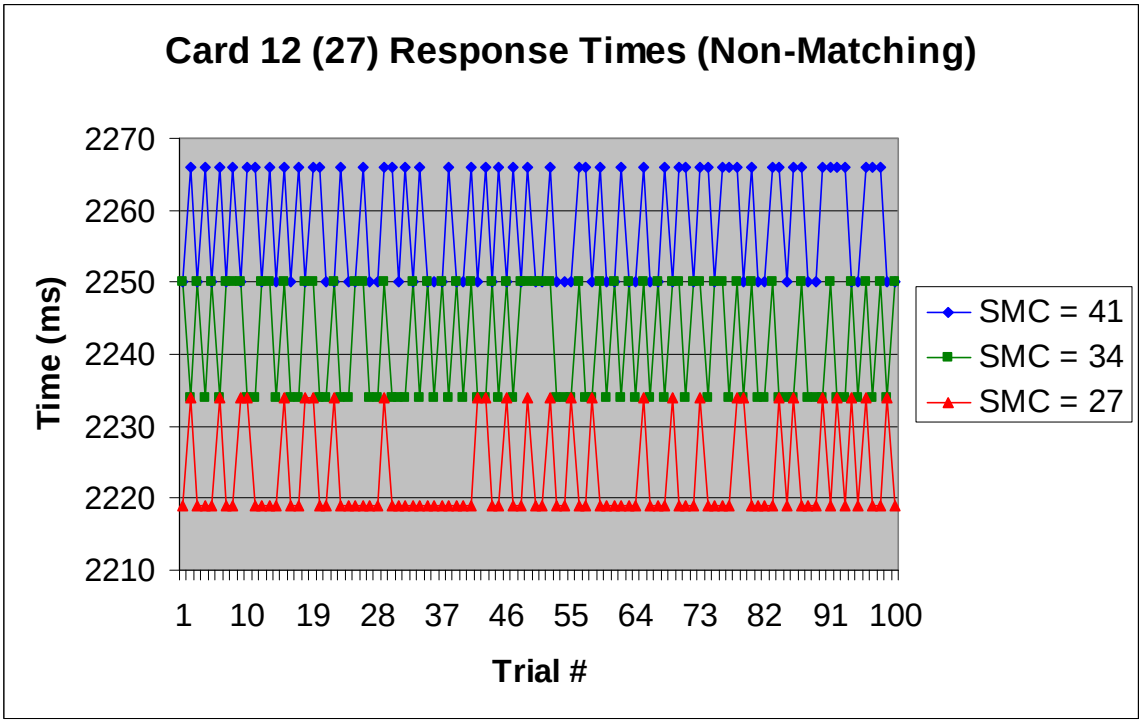


Figure C-64. Card 12 (27) Response Times for Non-Matching Templates

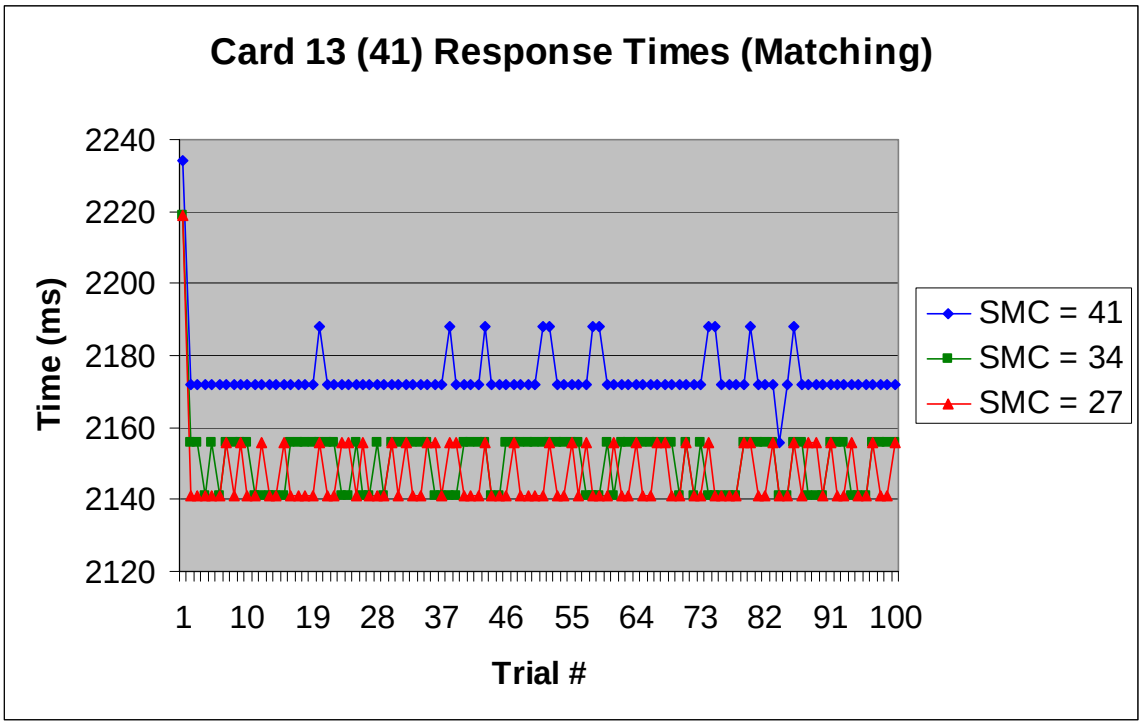


Figure C-65. Card 13 (41) Response Times for Matching Templates[9]

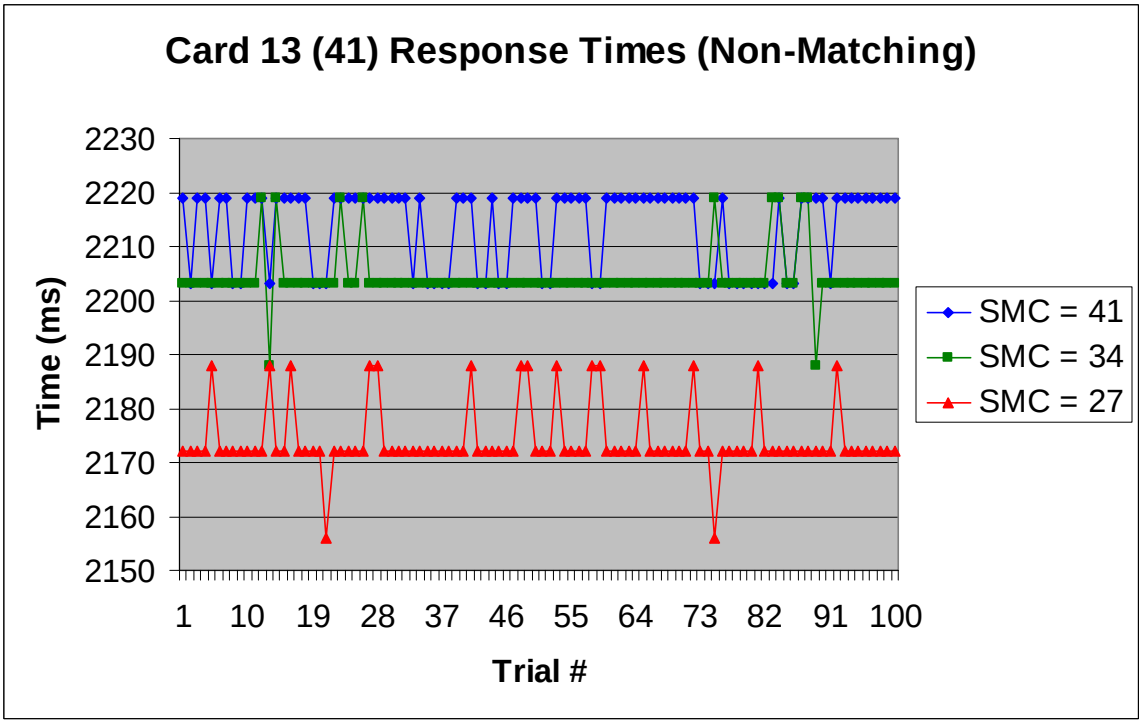


Figure C-66. Card 13 (41) Response Times for Non-Matching Templates

[9] Card 13 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

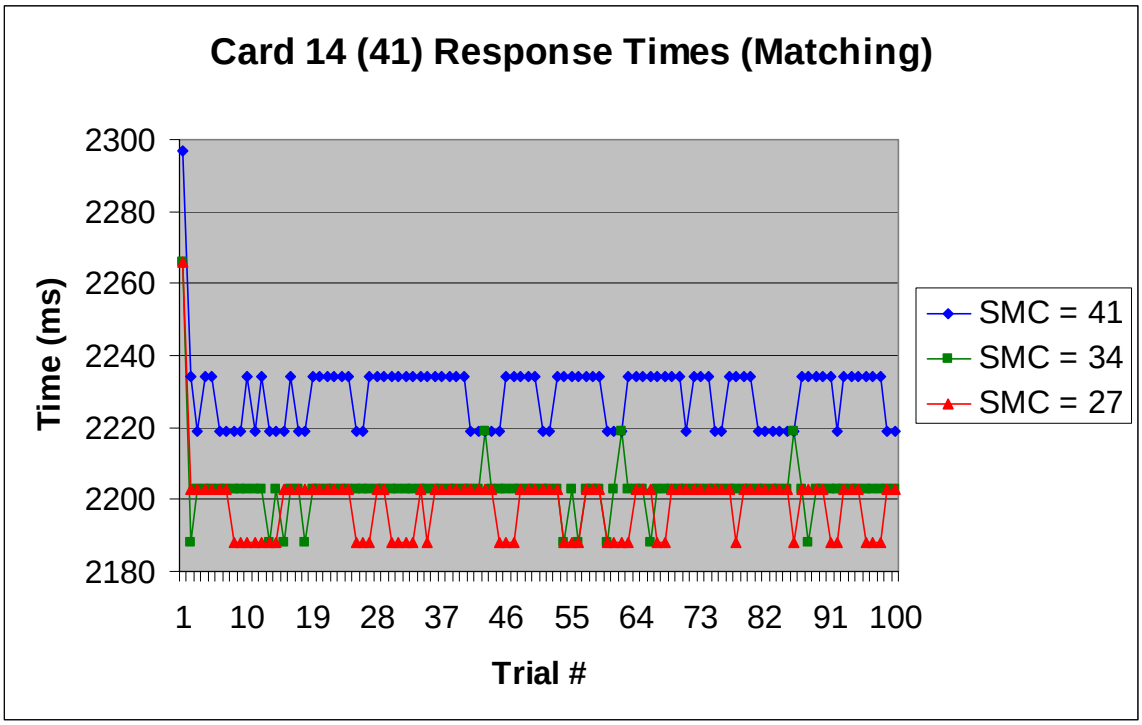


Figure C-67. Card 14 (41) Response Times for Matching Templates[10]

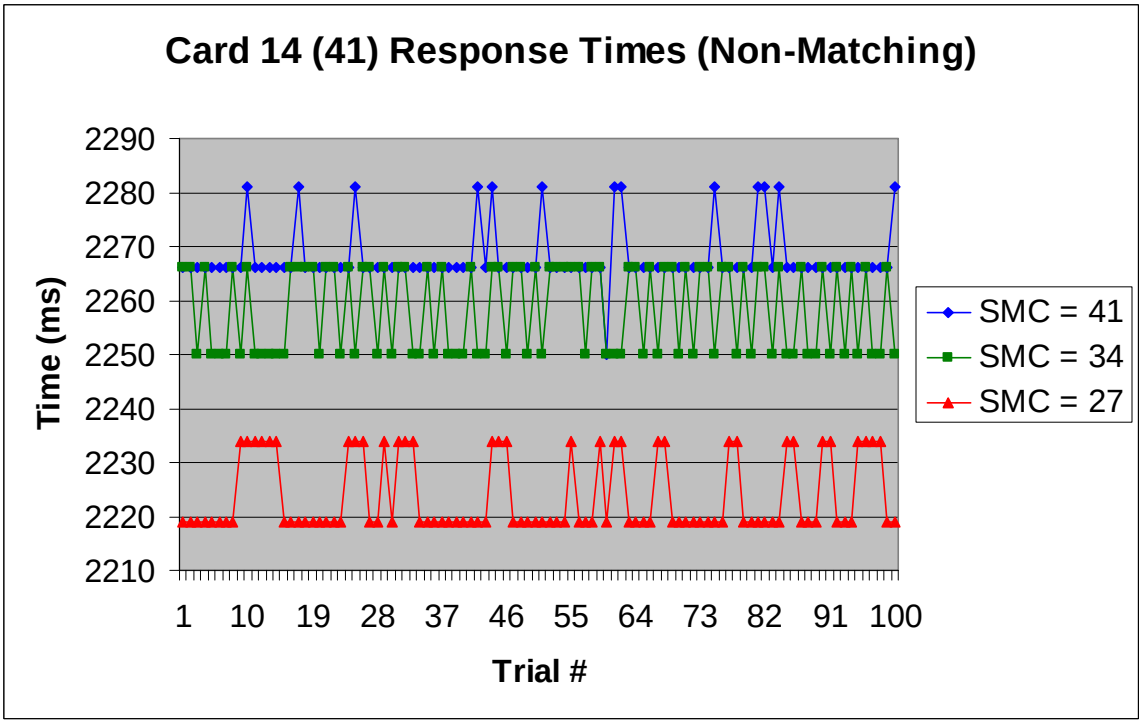


Figure C-68. Card 14 (41) Response Times for Non-Matching Templates

[10] Card 14 was loaded with a reference fingerprint template containing a proprietary extension and a minutia count of 41. It was not tested with reference fingerprint templates containing a minutia count of 34 or 27.

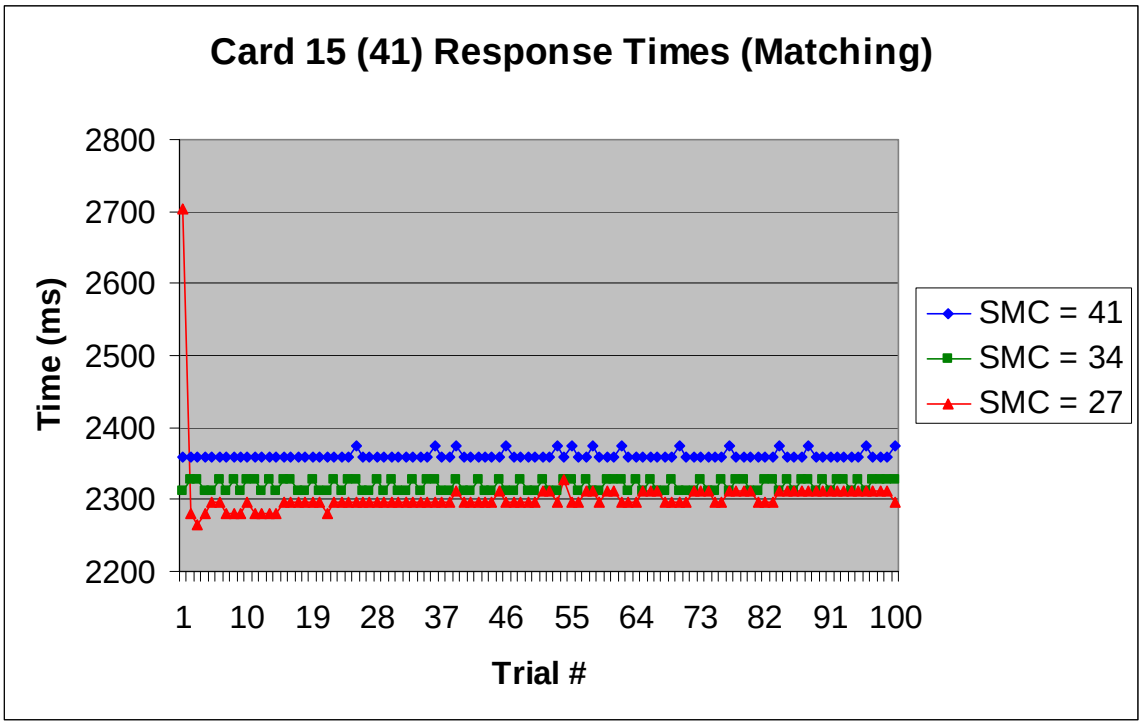


Figure C-69. Card 15 (41) Response Times for Matching Templates

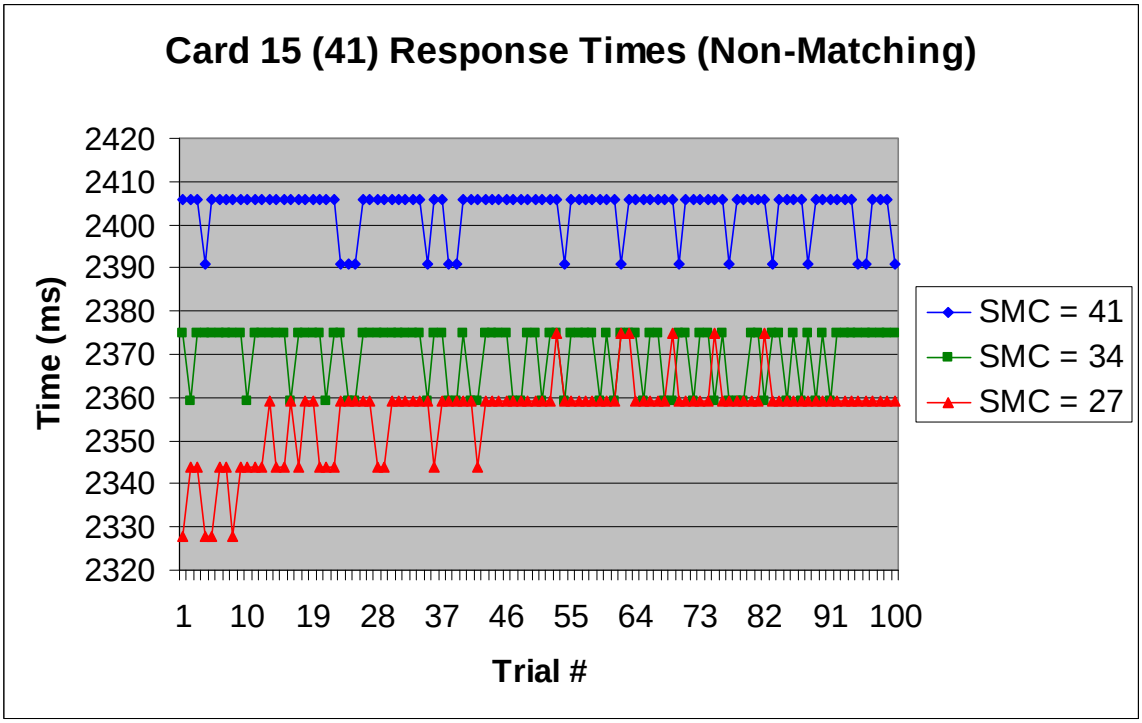


Figure C-70. Card 15 (41) Response Times for Non-Matching Templates

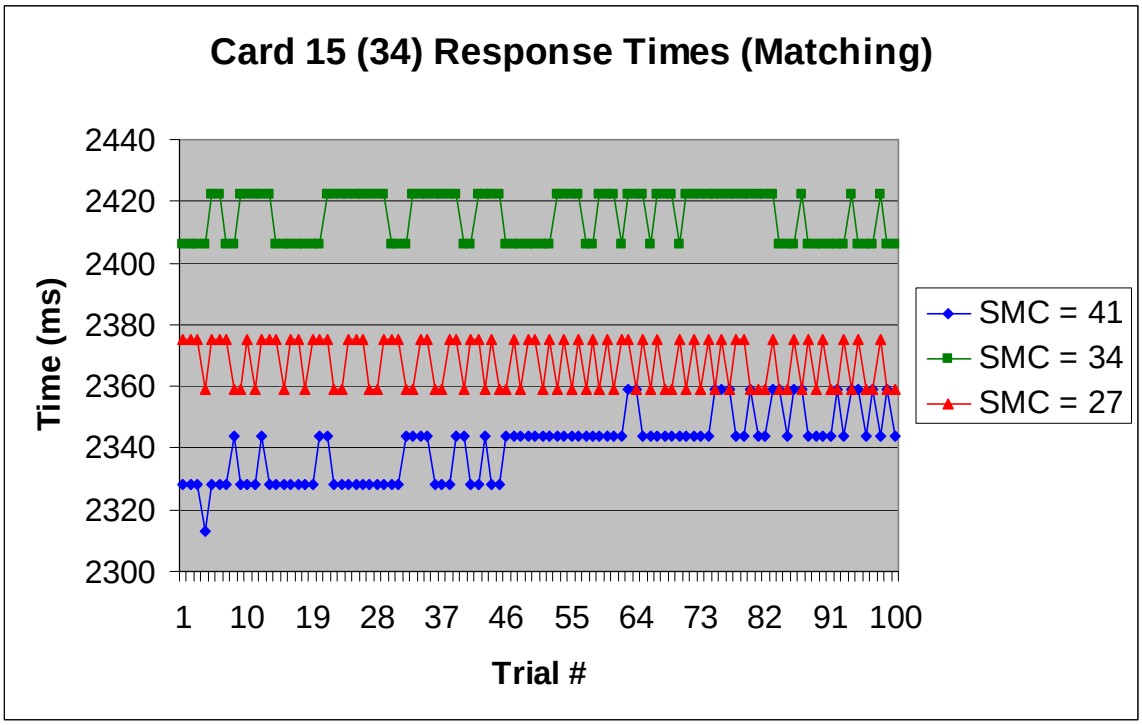


Figure C-71. Card 15 (34) Response Times for Matching Templates

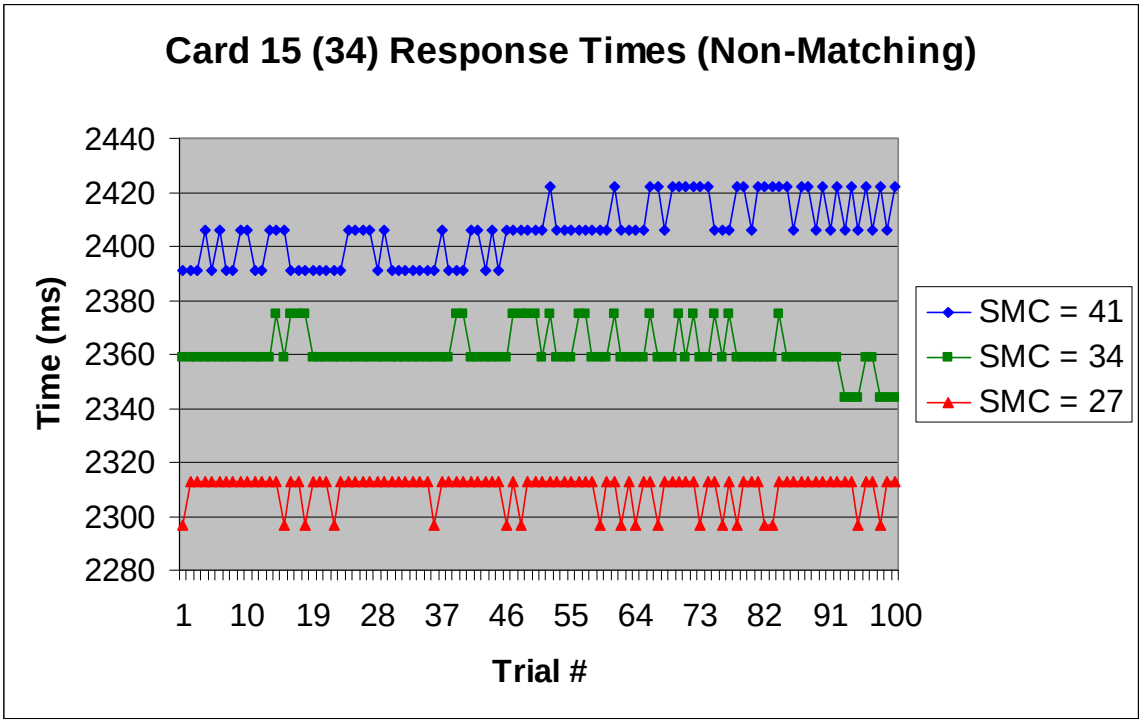


Figure C-72. Card 15 (34) Response Times for Non-Matching Templates

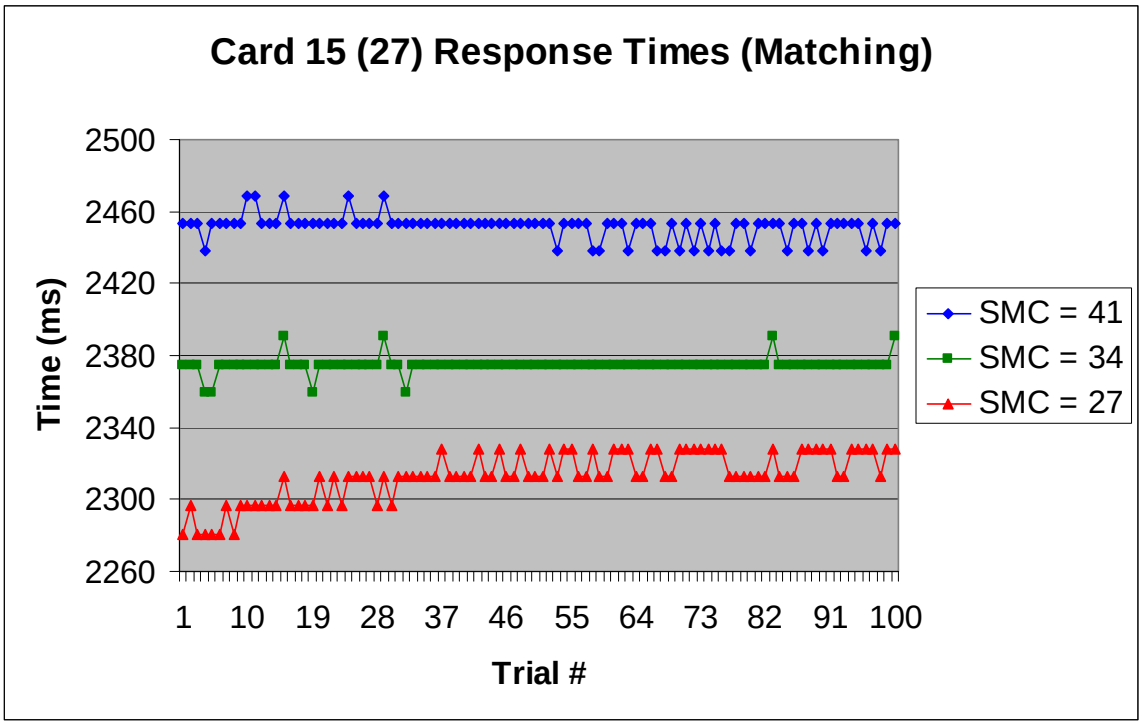


Figure C-73. Card 15 (27) Response Times for Matching Templates

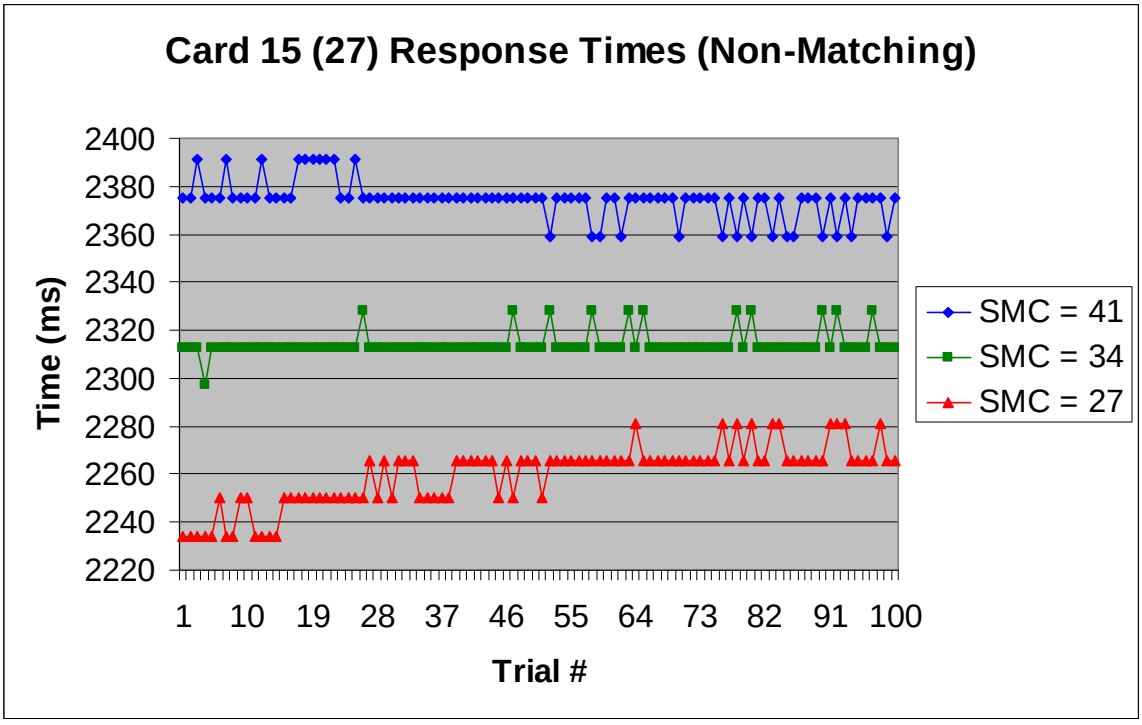


Figure C-74. Card 15 (27) Response Times for Non-Matching Templates

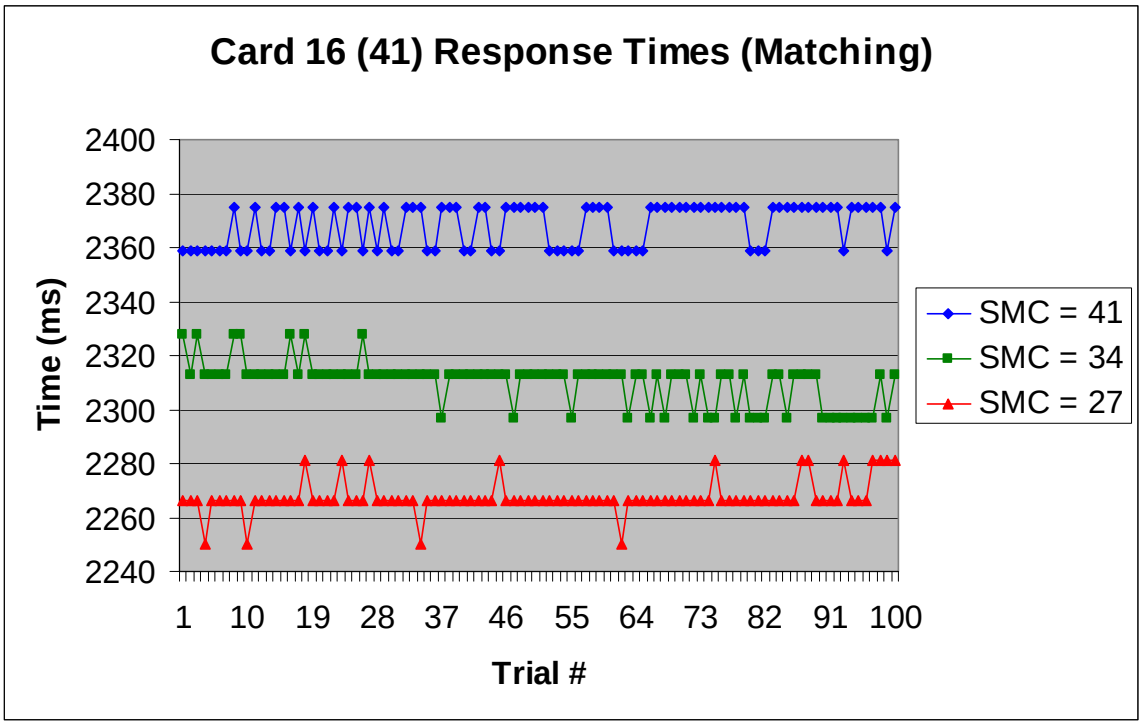


Figure C-75. Card 16 (41) Response Times for Matching Templates

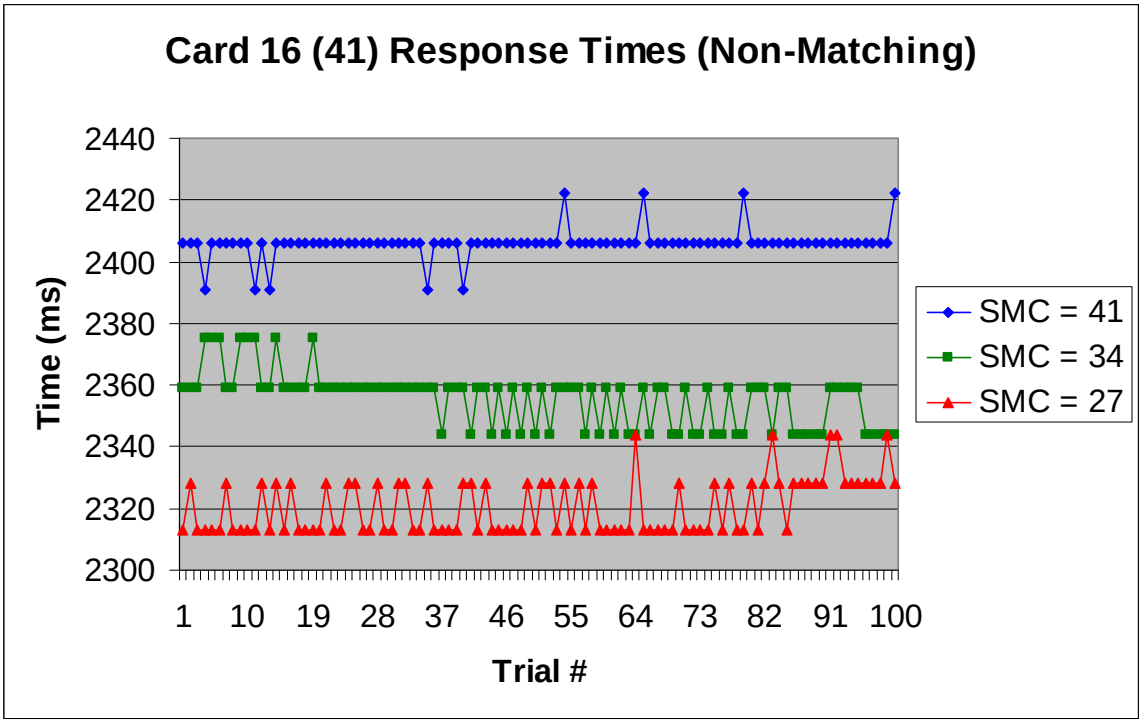


Figure C-76. Card 16 (41) Response Times for Non-Matching Templates

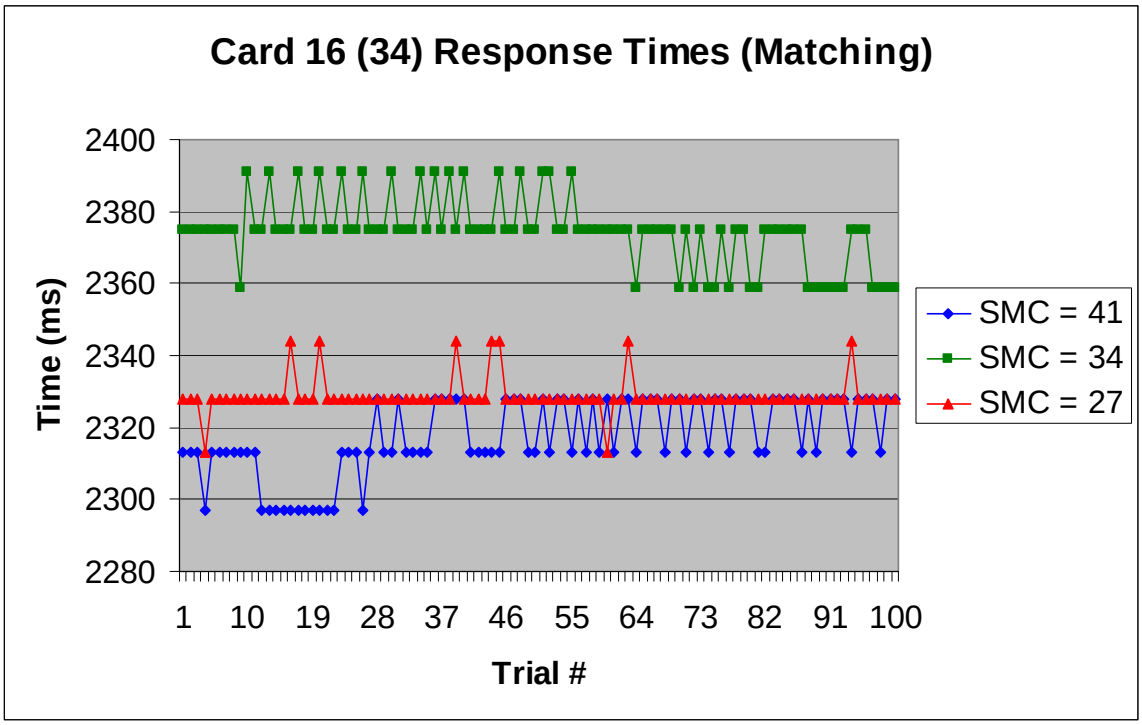


Figure C-77. Card 16 (34) Response Times for Matching Templates

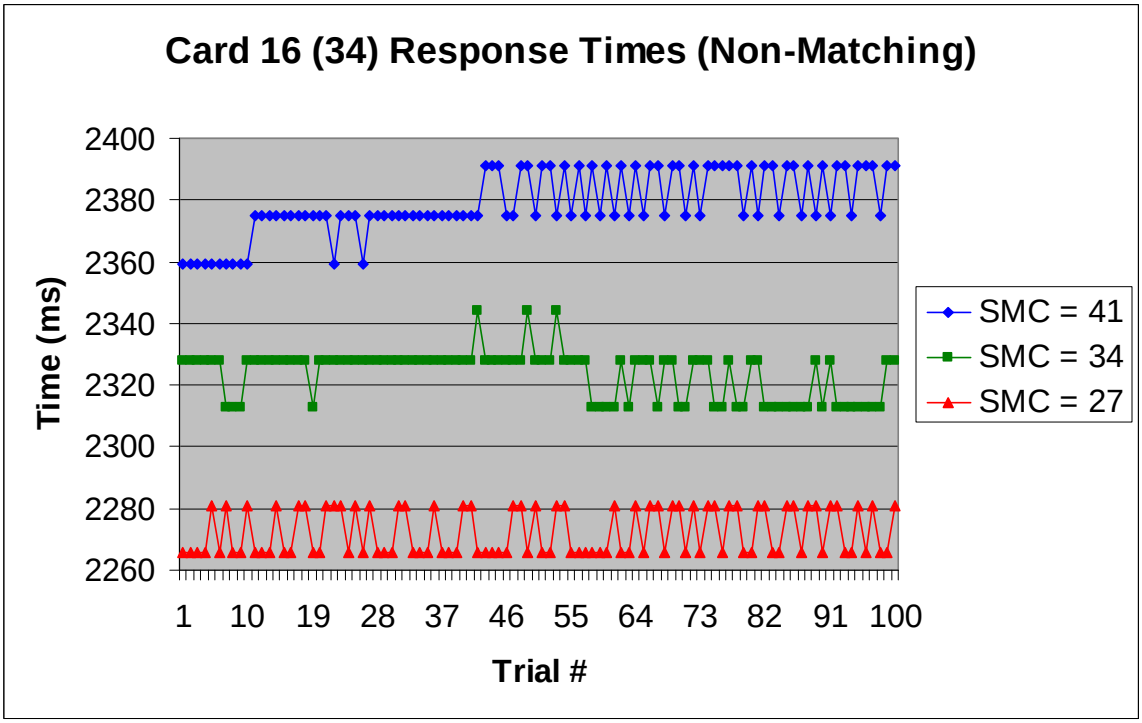


Figure C-78. Card 16 (34) Response Times for Non-Matching Templates

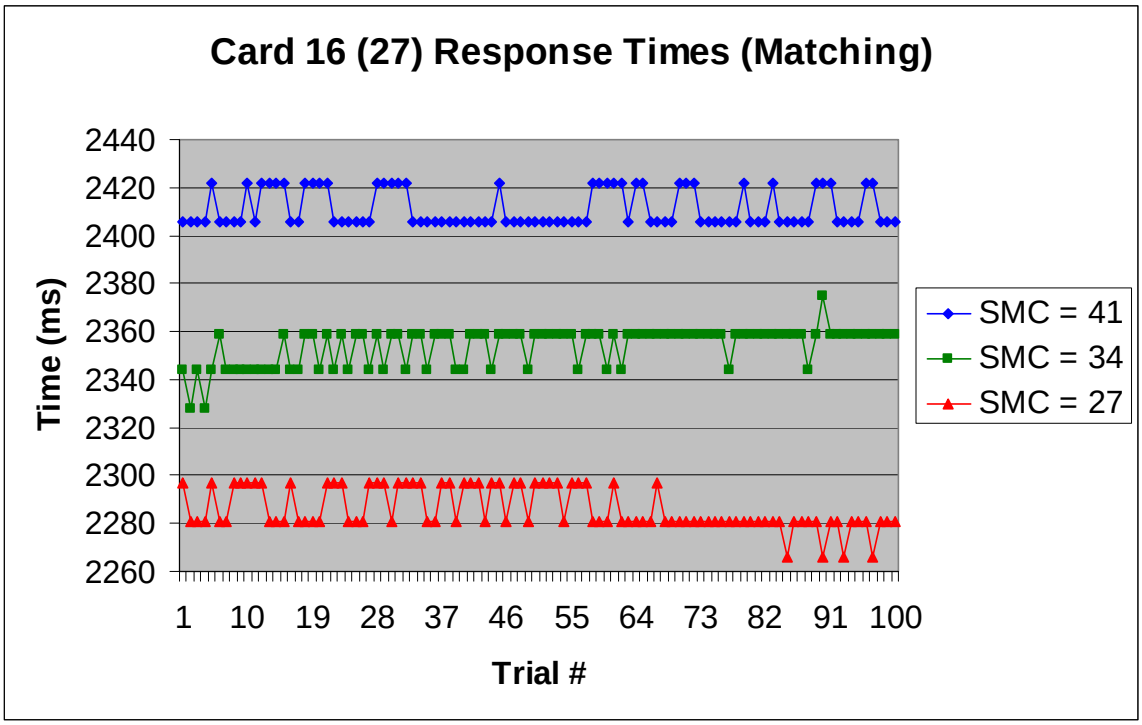


Figure C-79. Card 16 (27) Response Times for Matching Templates

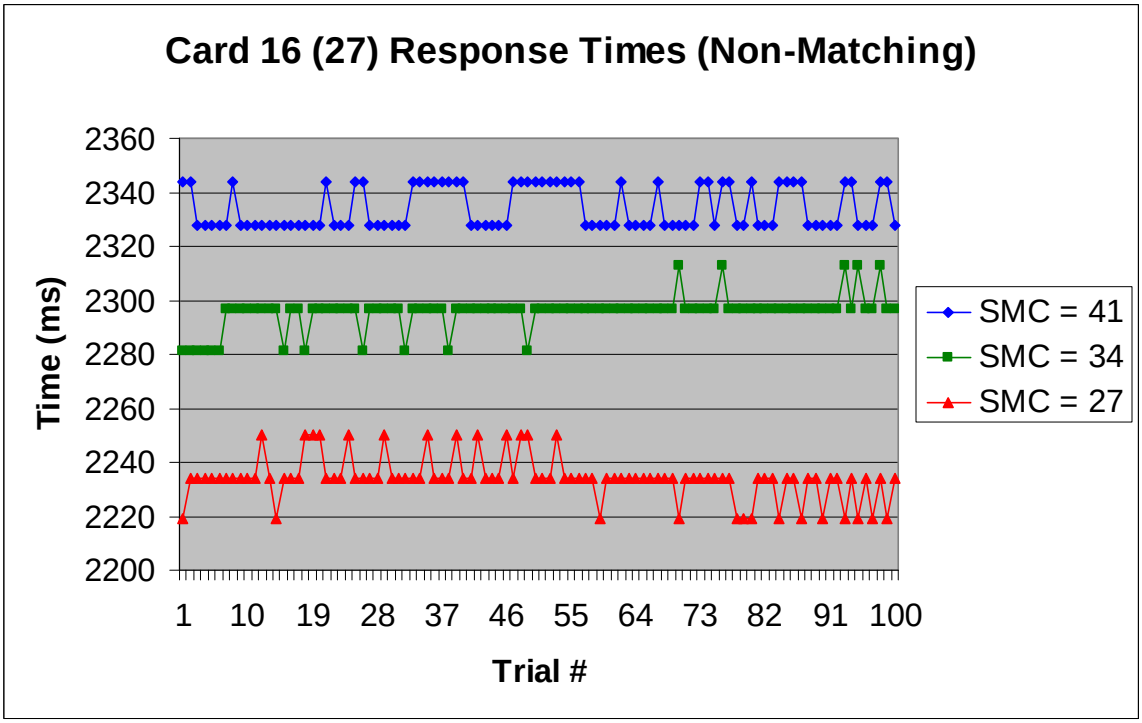


Figure C-80. Card 16 (27) Response Times for Non-Matching Templates

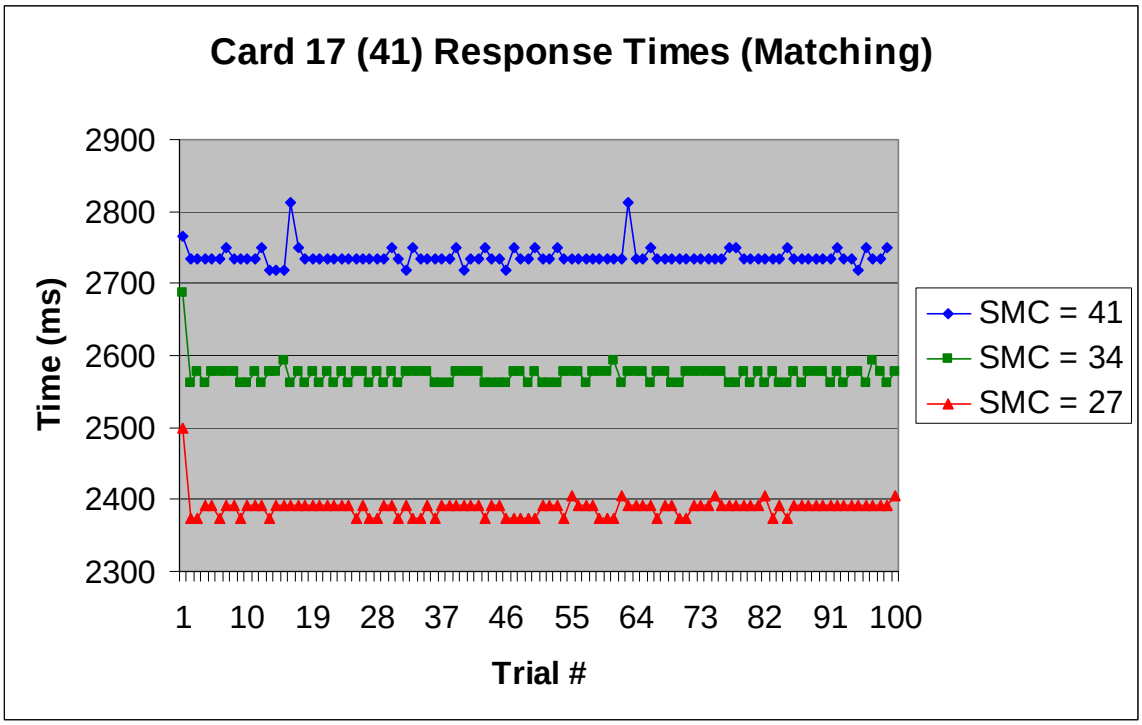


Figure C-81. Card 17 (41) Response Times for Matching Templates

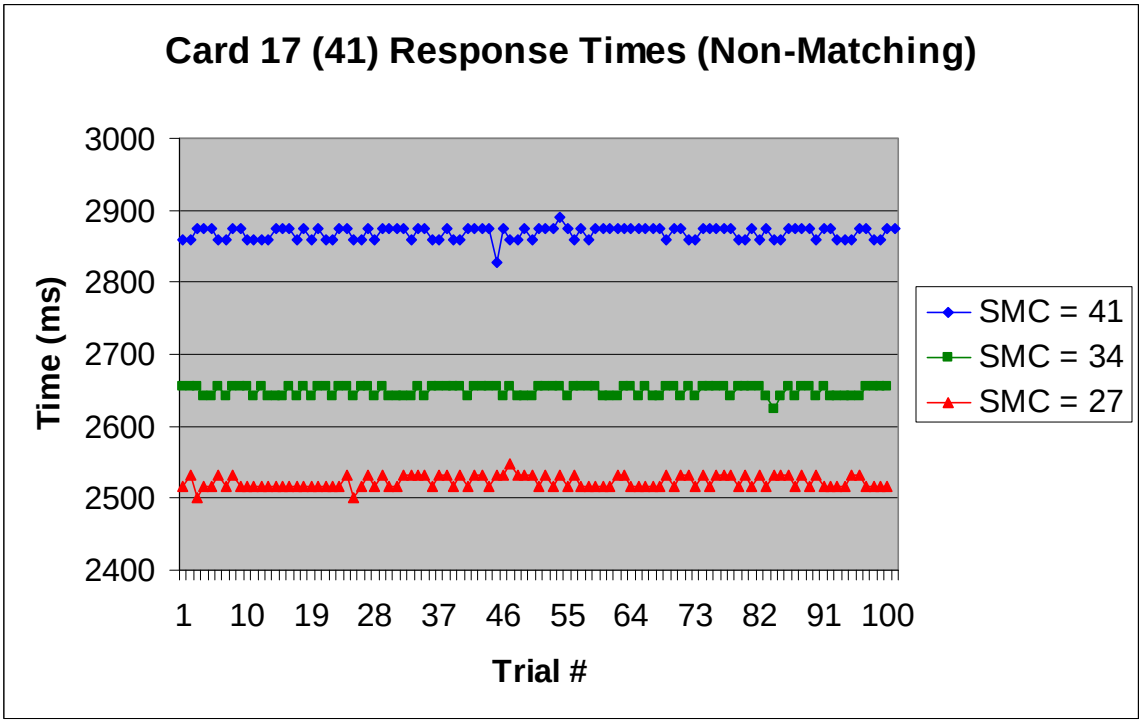


Figure C-82. Card 17 (41) Response Times for Non-Matching Templates

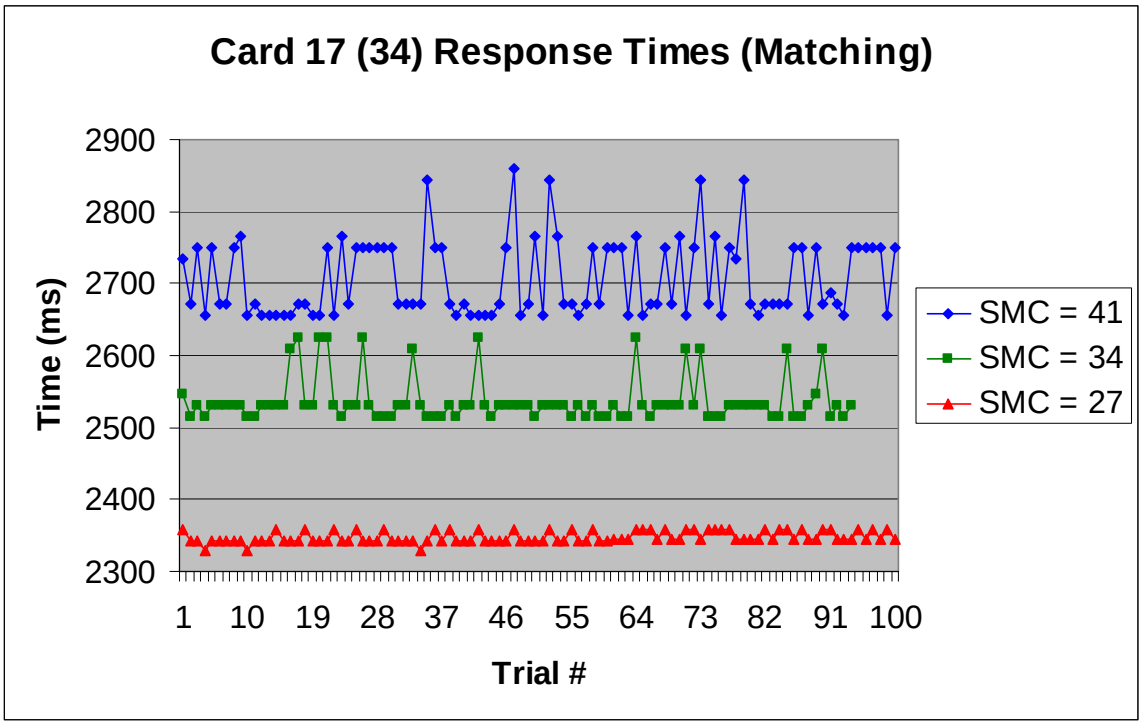


Figure C-83. Card 17 (34) Response Times for Matching Templates

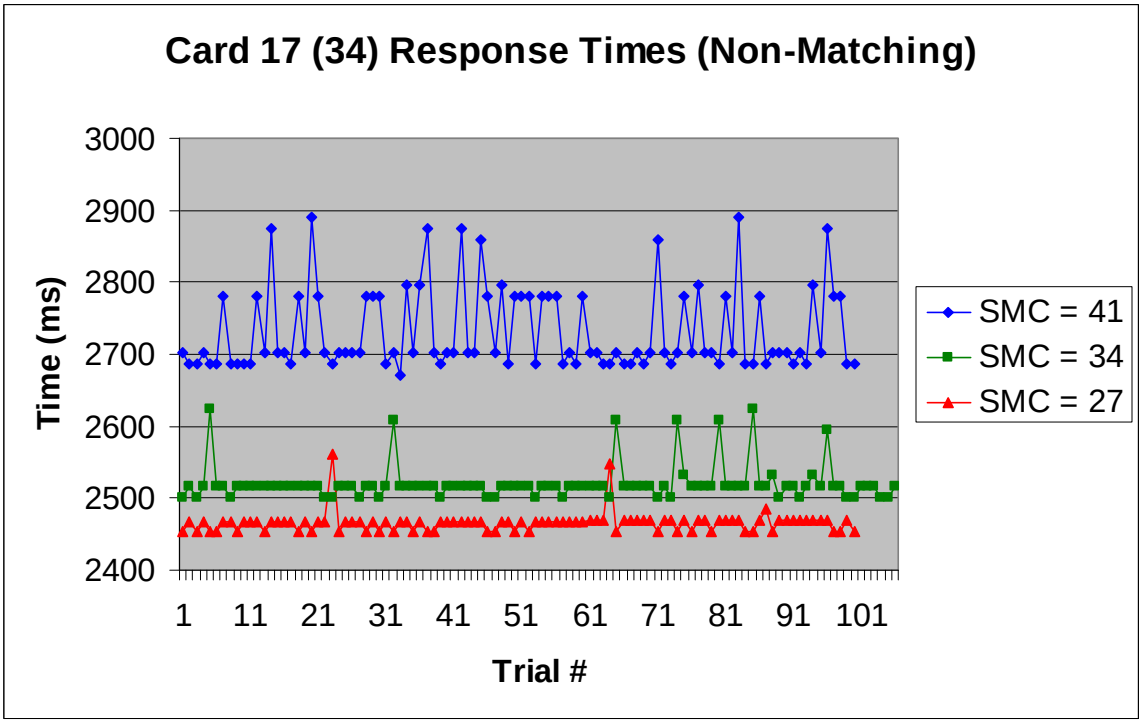


Figure C-84. Card 17 (34) Response Times for Non-Matching Templates

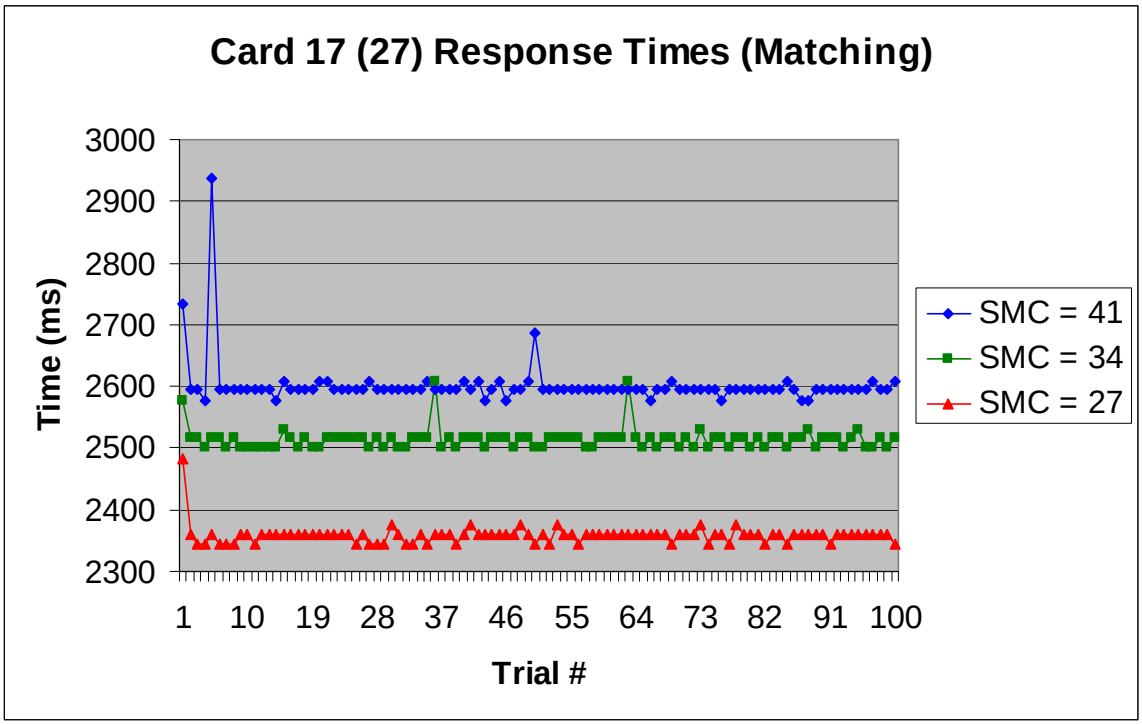


Figure C-85. Card 17 (27) Response Times for Matching Templates

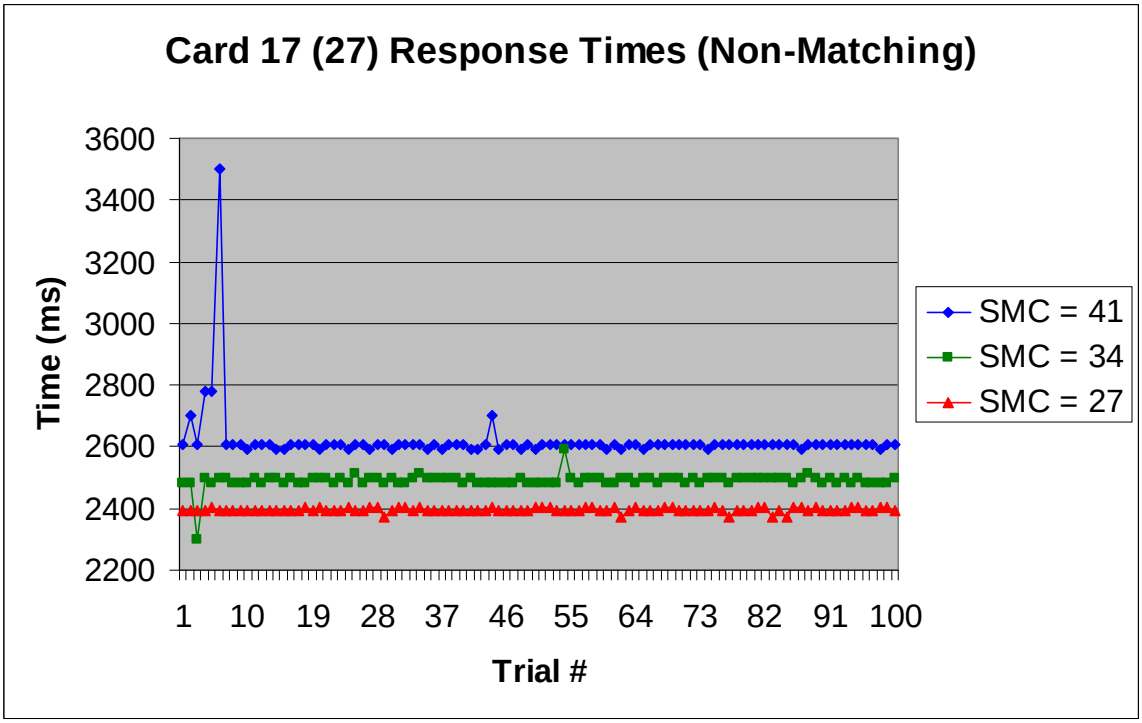


Figure C-86. Card 17 (27) Response Times for Non-Matching Templates

Appendix C—Sample Test Fixture Output

```
Date/Time,Run #,Reader,Card,Symmetric Crypto,Asymmetric Crypto,Fingerprint Filename,Finger,Minutia Count,Total Time,T0,T1,Cert
Verified,Finger Verified
09/13/07 15:12:28,1,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,859,595,172,Yes,Yes
09/13/07 15:12:29,2,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:12:29,3,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:30,4,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:31,5,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,172,Yes,Yes
09/13/07 15:12:32,6,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:33,7,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:12:33,8,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:34,9,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:35,10,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,203,Yes,No
09/13/07 15:12:36,11,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:37,12,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:12:37,13,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:38,14,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:39,15,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:12:40,16,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,579,203,Yes,No
09/13/07 15:12:41,17,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:12:41,18,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:42,19,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:12:43,20,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:44,21,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,610,172,Yes,Yes
09/13/07 15:12:45,22,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:12:45,23,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:12:46,24,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:47,25,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:12:48,26,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,188,Yes,No
09/13/07 15:12:49,27,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:50,28,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:12:50,29,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:12:51,30,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:52,31,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:53,32,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:12:54,33,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:54,34,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:55,35,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:12:56,36,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,579,203,Yes,No
09/13/07 15:12:57,37,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:12:58,38,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:12:58,39,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:12:59,40,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:00,41,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,594,156,Yes,Yes
```

```
09/13/07 15:13:01,42,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:02,43,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:02,44,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:03,45,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:04,46,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:05,47,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:06,48,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:06,49,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:07,50,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:13:08,51,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:09,52,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:10,53,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:10,54,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:11,55,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:12,56,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:13:13,57,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:14,58,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:15,59,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:15,60,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:13:16,61,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:17,62,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:18,63,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:19,64,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:19,65,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:20,66,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:21,67,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:22,68,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:23,69,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:23,70,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:13:24,71,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,172,Yes,Yes
09/13/07 15:13:25,72,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:26,73,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:27,74,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:27,75,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:13:28,76,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:13:29,77,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:30,78,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:31,79,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:32,80,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:13:32,81,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:33,82,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:34,83,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:35,84,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,203,Yes,No
09/13/07 15:13:36,85,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:36,86,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:37,87,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:38,88,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:39,89,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:40,90,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:13:40,91,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:41,92,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
```

```
09/13/07 15:13:42,93,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:13:43,94,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:44,95,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:44,96,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,203,Yes,No
09/13/07 15:13:45,97,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:46,98,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:47,99,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:48,100,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:48,101,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:13:49,102,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,203,Yes,No
09/13/07 15:13:50,103,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:51,104,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:52,105,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,610,172,Yes,Yes
09/13/07 15:13:53,106,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:53,107,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:54,108,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:55,109,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,610,172,Yes,Yes
09/13/07 15:13:56,110,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:57,111,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:13:57,112,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:13:58,113,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:13:59,114,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:00,115,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:01,116,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:01,117,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:14:02,118,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:03,119,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:14:04,120,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:14:05,121,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:05,122,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:06,123,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:14:07,124,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:14:08,125,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:14:09,126,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,203,Yes,No
09/13/07 15:14:10,127,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:14:10,128,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:14:11,129,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:12,130,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:13,131,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:14,132,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,203,Yes,No
09/13/07 15:14:14,133,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:15,134,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,188,Yes,No
09/13/07 15:14:16,135,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:17,136,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:18,137,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:14:18,138,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:19,139,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:20,140,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:21,141,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:14:22,142,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:14:22,143,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,610,156,Yes,Yes
```

```
09/13/07 15:14:23,144,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:24,145,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:25,146,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:14:26,147,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:26,148,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,203,Yes,No
09/13/07 15:14:27,149,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:14:28,150,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:29,151,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:30,152,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:31,153,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:31,154,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:14:32,155,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,156,Yes,Yes
09/13/07 15:14:33,156,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:34,157,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:35,158,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:14:35,159,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:36,160,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:37,161,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:38,162,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,203,Yes,No
09/13/07 15:14:39,163,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:39,164,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:40,165,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:41,166,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:42,167,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:43,168,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:43,169,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:44,170,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:45,171,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:46,172,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:47,173,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:47,174,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:48,175,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:49,176,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:50,177,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,579,172,Yes,Yes
09/13/07 15:14:51,178,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,188,Yes,No
09/13/07 15:14:52,179,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:14:52,180,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:53,181,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:54,182,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:55,183,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:14:56,184,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:56,185,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:14:57,186,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:14:58,187,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,595,156,Yes,Yes
09/13/07 15:14:59,188,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:15:00,189,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:15:00,190,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
09/13/07 15:15:01,191,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,156,Yes,Yes
09/13/07 15:15:02,192,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,610,188,Yes,No
09/13/07 15:15:03,193,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:15:04,194,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
```

```
09/13/07 15:15:04,195,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:15:05,196,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,610,203,Yes,No
09/13/07 15:15:06,197,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,781,610,156,Yes,Yes
09/13/07 15:15:07,198,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,813,595,203,Yes,No
09/13/07 15:15:08,199,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserL2_41_sample.iso-fmc-cs,Left index,41,797,595,172,Yes,Yes
09/13/07 15:15:09,200,Reader A,Card 1 (41),2 Key TDES - ECB,RSA 1024,UserR3_41_sample.iso-fmc-cs,Right middle,41,828,595,203,Yes,No
```

Appendix D—Test Approach

D.1 Purpose

FIPS 201-1 and associated NIST Special Publications define a method to perform biometric authentication of a PIV cardholder when the PIV Card is inserted into a contact smart card reader. In some use cases, however, contactless operation is required. Security concerns have hindered communication of biometric data transfer over the contactless interface. The transaction data can be protected by secure messaging and data encryption, but these methods can impact performance. To understand the effects of security on performance, NIST will conduct a technical feasibility study of secure data transfer over the contactless interface to perform Secure Biometric Match-On-Card (SBMOC) operations. Eventually, NIST may propose an extension of the FIPS 201 standard that achieves secure biometric authentication in the contactless mode of operation, but such a proposal is not an immediate goal of this study.

The study will use PKI to create an authenticated, secure session (like an SSL/TLS session) that protects the integrity and confidentiality of messages sent from the terminal to a smart card, and the integrity and authenticity of messages sent from the smart card to the terminal. The protocol never releases biometric data from the smart card, called the Device Under Test (DUT) in this document. Instead, the DUT receives an encrypted sample template from a biometric reader, performs a match against a reference template stored on the DUT, and returns a logically signed Yes/No result to the reader.

Preliminary tests of BMOC operation have shown that a BMOC operation for physical access could be performed within 500 milliseconds without secure messaging. Tests of PKI transaction times suggest that the approach could meet a success criterion of less than 2.5 seconds per transaction.

D.2 Security Objectives

FIPS 201-1 permits biometric data to be released only across the contact interface of a PIV Card, and only after activation of the PIV Card through presentation of the cardholder's Personal Identification Number (PIN). These restrictions achieve two security objectives: communication of biometric data occurs only over a trusted communication channel that is not easily subject to eavesdropping attacks (namely, the wired contacts inside the smart card reader); and the PIV cardholder implicitly attests to the legitimacy of the smart card reader, as they indicate by entering the PIN on the smart card reader keypad. FIPS 201-1 enables biometric authentication to occur without imposing a technical requirement for automatic authentication of smart card readers to PIV Cards. Such a requirement, it was believed, would add unacceptable key management costs. (The PIV fingerprint object is digitally signed, and the signature can be used to verify authenticity and integrity of the data.) This feasibility study will evaluate the impact of a secure protocol on transaction performance, when the protocol meets these security objectives:

+ SO1: communication of biometric data shall occur only over a trusted channel that is not susceptible to eavesdropping attacks in the reader-to-card direction, nor spoofing or replay attacks in the card-to-reader direction; and

+ SO2: communication of biometric data between the smart card and smart card reader shall occur only after the cardholder has indicated the reader is legitimate; and

+ SO3: communication of biometric data from the smart card to the reader shall occur only after the cardholder has entered their PIN; and

+ SO4: the approach should achieve the preceding security objectives without reader-to-smart-card authentication or associated key management infrastructure.

These security objectives are aligned with the high-level security objectives of FIPS 201-1. They protect both the integrity of the biometric authentication transaction and the privacy of the cardholder's biometric data, while avoiding the potential cost of reader authentication key management.

D.3 Functional and Performance Objectives

The Device Under Test (DUT) shall be a smart card having ISO/IEC 7810 physical and mechanical characteristics.

The Device Under test shall be capable of contact (via ISO/IEC 7816-3 methods, consistent with NIST SP800-73-1) and contactless (via ISO/IEC 14443 methods, consistent with NIST SP800-73-1).

Preferably, the DUT is listed on the General Services Administration (GSA) HSPD-12 Approved Product List, and modified only by the addition of BMOC firmware. The DUT may also be a type of smart card not on the GSA Approved Product List (APL). In this case, NIST will determine if the DUT could host a PIV card-application at reasonable development cost, and if so, the DUT will be tested.

The DUT may not have an NPIVP or a Cryptographic Module Validation Program (CMVP) certificate. In this case, NIST will determine if the DUT could pass NPIVP and CMVP testing at reasonable development cost, and if so, the DUT will be tested.

The DUT should perform a Biometric Match-On-Card authentication transaction and meet the security objectives described in Section D.2.

The biometric matching algorithm on the DUT should demonstrate accuracy meeting the criteria of SP800-76-1 Section 8.10 by testing in either the NIST MINEX II or Ongoing MINEX activity. (Note: accuracy testing may run concurrently with performance and security testing.)

The fingerprint sample template sent from the reader to the DUT should be represented following either ISO 19794-2 finger minutiae card or ANSI 378 format. Any extensions or options must be fully documented in the submitted protocol documentation.

Both RSA 1024 and RSA 2048 should be available as asymmetric algorithm alternatives unless one of these is not available on the DUT.

AES (preferred), 3TDEA, or 2TDEA (deprecated) should be implemented at the symmetric encryption algorithm.

The target transaction time for the SBMOC Technical Feasibility Study is 2.5 seconds or less and is measured from steps 2 through 10 in Section D.5. Performance will be measured and reported separately for matching and non-matching cases.

D.4 Test Plan

This test plan identifies the tasks necessary to design, develop and install the BMOC Performance Test Platform at the NIST test facility located in Gaithersburg, MD.

The submission package to NIST will include:

+ An executed copy of the Materials Transfer Agreement;
+ Documentation of the ISO/IEC 7816 command sequence implementing the SBMOC protocol, and at least one complete protocol sequence as an example;
+ Three DUTs (smart cards) capable of performing the SBMOC protocol;
+ Documentation of the loading process for biometric templates onto the smart card, both initially and as a replacement after the initial load.

Additional software tools or examples maybe supplied with the submission package.

Once a complete submission package has been received, NIST will begin a security analysis of the SBMOC protocol to determine if it meets the security-related objectives of Sections D.2 and D.3. NIST will construct the client-side protocol implementation in the test framework. NIST will develop a new client-side protocol implementation for each submitted DUT (this will insure that NIST is able to construct working client-side software from the protocol documentation).

The test fixture will record the duration of each command-response transaction between the host and the card. A test record will therefore contain a complete log of all APDUs exchanged, and timing on each request-response pair individually. A trial will run tests and reference templates, and with non-matching sample and reference templates, to highlight any differences in transaction time arising form the match result. If the reference template object contains multiple templates, trials will be designed to disclose the effects of multiple templates (e.g., separate trials matching first template vs. second on variance, break down communication and processing time per request-response cycle, document the amount of data transmitted (in both directions) during the protocol scenario, and estimate the command-response time per sub-activity (e.g., “read certificate, “general authenticate”, “verify”).

D.5 Protocol Implementation

The performance tests will measure the duration of phases during the SBMOC transaction. The rationale for the approach relies on two observations. First, the PIV System trust model is founded on PKI, and by design, any PIV Card can authenticate itself to another system element at a medium high assurance level using a private key and certificate stored on the card. Second, if a biometric match operation is performed on the PIV Card using SBMOC technology, there is no need to release biometric data from the PIV Card to any other system element (thus satisfying SO3 in Section D.2).

Variations in protocol implementation are acceptable provided that the objectives in Sections D.2 and D.3 are achieved.

In outline, the use scenario is as follows. The cardholder presents their card to a contactless biometric reader, and presents their finger to the biometric scanner. The scanner obtains a fingerprint image which is transformed into the sample template, encrypted, and transmitted via contactless into the PIV Card. The PIV Card decrypts the template, matches the sample template against the reference template stored on the PIV Card, and returns a signed “Yes” or “No” result to the smart card reader.

An example of a more detailed protocol is included next.

1. The cardholder presents their PIV Card to the contactless smart card reader.
2. The host system selects the SBMOC application on the card.

`e.g., using the SELECT APDU`

3. The smart card reader performs Get Data to read the PKI certificate from the PIV Card, and validates the PKI certificate.

   `e.g., using the GET DATA APDU followed by GET RESPONSE APDU(s)`

4. The host system gets the nonce (a random card data) from the card. The card responds with 8-bytes Rc(1) and 16 bytes Rc(2). Rc(1) is used to authenticate the host and Rc(2) is used to derive the session keys.

   `e.g., using the GET CHALLENGE APDU`

5. The card and host system generate encryption and MAC session keys.

   GENERAL AUTHENTICATE – Used to communicate the session keys in an ciphered data block encrypted by the card public key. The encryption uses the following input data:

   - Random number for encryption session key (PSKenc)– 16 bytes
   - Random number for MAC session key (PSKmac) – 16 bytes
   - Rc(1) – 8 bytes padding received from GET CHALLENGE APDU
   - PKCS #1 padding

   GENERAL AUTHENTICATE returns the encryption and MAC session keys.

   `e.g., using the GENERAL AUTHENTICATE APDU`

6. A secure session is established between the card and the host system. Both the card and the host system use the Rc(2) as a key to compute encryption session key and MAC session key. The algorithm is: SKmac = 3DES(PSKmac, Rc(2)) and SKenc = 3DES(PSKenc, Rc(2)).
7. The cardholder presents their finger to the fingerprint scanner.
8. The fingerprint scanner scans the finger, and generates the sample template from the image. Alternatively, the finger print template is retrieved from a file.
9. The smart card reader encrypts the sample template using the session encryption key.
10. The host system sends the template to the card for authentication

    - VERIFY – Used to send encrypted biometric template for authentication. The input data should be of the following format: 0x7F 0x2E || length || 0x81 || length || encrypted biometric template (pad the template with zero at the end to make it multiple of 8 bytes. The response of 90 00 means the biometric template matched. The message also responds with 9 bytes of MAC for further verification by the host system.

```
e.g., using the VERIFY APDU
```

The time to complete each of the request-response transactions, and the total time to complete steps 2-10 will be recorded. Repeated measurements will be made to estimate variance. Trials will be conducted with templates that match, and with templates that do not match. The public key algorithm used will be RSA, and trials will be conducted at 1024 and 2048 bit key lengths.

D.6 Publication of Results

A submission is successful if it achieves the objectives in Sections D.2 and D.3 when tested. At the completion of testing, NIST will publish a summary report indicating the number of successful submissions, and for each successful submission, and for both RSA 1024 and 2048, and for matching and non-matching tests:

1. the average total time for the transaction;
2. average time to establish a secure session;
3. average time to transmit the reference template to the smart card;
4. average time to compute the match;
5. average time to transmit the result from the smart card;
6. whether or not the smart card has passed NPIVP testing;
7. whether or not the smart card has passed CMVP testing.

The average total time (1) will be approximately (2) + (3) + (4) + (5).

NIST may also publish summary observations and recommendations resulting from the protocol security analyses, without reference to specific submissions.

In conformance with the “no endorsement” policy of NIST, the names of participants will not be published.

Appendix E—Acronyms

The following acronyms and abbreviations are used throughout this document:

2TDEA	2-Key Triple Data Encryption Algorithm
3TDEA	3-Key Triple Data Encryption Algorithm
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programming Interface
APL	Approved Product List
CBC	Circular Binary Coding
CMVP	Cryptographic Module Validation Program
CSV	Comma-Separated Values
DES	Data Encryption Standard
DUT	Device Under Test
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
MAC	Message Authentication Code
MINEX	Minutiae Interoperability Exchange Test
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NPIVP	NIST's Personal Identity Verification Program
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RF	Radio Frequency
RSA	Rivest Shamir Adleman
SBMOC	Secure Biometric Match-on-Card
SMC	Sample Minutia Count
SP	Special Publication

Appendix F—References

[1] HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

[2] Federal Information Processing Standard 201-1, Change Notice 1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006. (See http://csrc.nist.gov)