GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
Scenario 1: System Access and Compatibility			
1	User is able access the system using an iOS device (tablet and iPhone).	The system is **accessible** and functional using the following versions of the Safari web browser on iOS: 7.0 through 7.1.6 and 8.0 through 8.0.6.	1,3
2	User is able to access the system using an Android device (tablet or phone) using the Kit Kat and Lollipop versions of the Android OS. For the purposes of the Live Test Demonstration, only the KitKat and Lollipop versions of the Android OS will be required for demonstration but this does not limit the scope of the requirement.	Based on the Government provided equipment, supporting operating systems and browsers, the EAS is **accessible** and functional using the following Android operating systems: KitKat (4.4–4.4.4, 4.4W–4.4W.2) Lollipop (5.0–5.1.1).	1,4
3	User is able to access the system using Windows XP, Vista, and Windows 7.	Based on the Government provided equipment, supporting operating systems and browsers, the EAS is **accessible** and functional using the following of the Safari web browser 4.03 through 4.05 in addition to 5.0 through 5.17; Internet Explorer versions 7.0 through 11.x; Google Chrome; and Firefox.	1,5
Scenario 2: Account Set-up and User Options			

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
4	User can create a User Name and Password to access the EAS.	The user should be able to create a User Name and a password that is 'strong' which is at least 12 characters in length and consist of the following: -Does not contain all or part of the user's account name -Contains characters from at least three of the following categories: English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non alphabetic characters (for example: !, $, #, %) If the user uses a 'bad' password that meets the 'strong' password criteria the system will reject it. The passwords are verified twice before being accepted.	6, 7, 8
5	System will not allow a user to enter the EAS with a bad password; and that if a bad password is used on five consecutive attempts in a 60 minute period the account is locked.	Only a user with a valid user name paired with the correct password can gain entry to the EAS and view their SmartPay account details. Further, it will be demonstrated that after five (5) unsuccessful attempts using a bad password for the same user name within sixty (60) minutes, the account is locked. Locked accounts can only be unlocked by calling a Customer Service representative. In the event a cardholder can't reach a Customer Service representative, the A/OPC shall have the ability to unlock accounts without having to ask validation questions of the cardholder. The system will prompt the user when their account is locked. The system shall generate a unique and secure incident ID number to include in the email to the account holder. The system shall email instructions on how to unlock the account to the email addresses on file for the account holder. In addition to validating the account holder information, Customer Service representative must verify the incident ID number provided before unlocking the account. The system shall send a Notification of locked accounts to the A/OPC or authorizing official of the designated agency personnel the account belongs to. The A/OPC shall have a reset account protocol or process to unlock the account from the EAS without having to use customer service. Notification of locked accounts will be sent to the authorizing official of the customer agency the account belongs to	9, 10, 11

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
6	User must change their password every 90 days.	Passwords must be changed every 90 days, with no exception. a) Remind users that passwords have expired and must be changed; b) Begin prompting password change 15 calendar days before passwords expire; c) If users fail to change passwords on the 15th day, at the end of the 90 calendar day cycle, the account will be locked.	12
7	User can change their password, at any time.	A user can change their passwords at any time while the account is unlocked.	13
Scenario 3: System Help			
8	Access the system help resources from anywhere in the application.	The EAS shall have context sensitive help for all pages of the application. The user shall have the ability to search for help topics, key words, and have flyover text available that also serves as a resource link to system help. The EAS shall have a user manual(s) accessible from within the system application and available for download.	15, 16
Scenario 4: Searching for User Accounts			
9	User with the appropriate role(s) can search for accounts using the following criteria: Name, Account Number, Employee ID, or Managing Account Number.	The EAS shall allow for authorized users to search for accounts by name, account number, employee identification, billing account number, or transacting account.	18

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
10	User with the appropriate role(s) can search for accounts using a First Name and Last Name.	The EAS shall allow for authorized users, as identified by the agency / organization within their span of control, with permission, the capability to search for accounts with a first name and last name. a) When the search is conducted with the first name only, all accounts within that customer agency will be listed with the first name specified. b) When the search is conducted with the Last Name only, all accounts within that customer agency will be listed with the last name specified. c) When the search is conducted with both first name and last name, all accounts within that customer agency will be listed with the first name and last name combination specified. The EAS should have the ability to conduct a wild card search based on wild card characters (e.g. “*”, “@”).	19
11	User is able to log off the EAS.	The EAS shall have a logoff capability to end user sessions. When a user logs off, the EAS will not store any data on devices, including but not limited to temp files, trackers, or other metadata.	20
Scenario 5: Maintain User Options			
12	User can update the organizational roles and levels/fields that the EAS provides as choices or default settings.	The EAS shall allow for A/OPCs and card managers to specify a default setting for organizational levels/fields.	21
13	Authorized user can DELETE a user account.	The EAS shall allow authorized users to delete assigned user accounts.	22
14	Authorized user can update another users profile and roles.	The EAS shall allow authorized users to update the profile and roles of the accounts for the assigned user’s accounts.	23

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
15	Authorized user can set the access levels for the user roles of an agency/organization. .	The EAS shall allow authorized users the ability to establish access levels.	24
16	Field level validation is in place and that the EAS displays error messages to the user.	The EAS shall have field level validations. Users shall be notified for incomplete fields following validation checks.	25
17	Functionality allows for new card requests.	The EAS shall have the capability to allow users to request a new charge card. Authorized users shall have the ability to initiate this request in the EAS.	26
Scenario 6: User Access and Maintenance Restrictions			
18	User can set user access and maintenance restrictions.	The EAS shall allow for users to set access and maintenance restrictions for the user accounts they manage.	27
19	User can verify access and maintenance restrictions	The EAS shall allow for users to verify access and maintenance restrictions set for the accounts they manage.	28
20	Authorized user can establish user profiles and assign roles to the users they manage.	The EAS shall allow account managers to edit the user profile of the accounts they manage and set change profile settings and assign user roles.	29
21	Authorized user can create a new user profile.	The EAS shall allow authorized users to create new user profiles, in a manner outlined at the agency/organization task order level requirements. .	30

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
22	Authorized user can create a new managing account.	The EAS shall allow authorized users to create new managed accounts.	31
23	Authorized user can create a new cardholder account from scratch or from a user profile.	The EAS shall allow authorized users to create new accounts or generate new accounts from user profiles.	32
24	Authorized user can verify status of submitted account applications.	The EAS shall provide a mechanism for authorized users to view the status of submitted account applications for both IBAs and CBAs.	33
Scenario 7: Verify Cardholder and Management Account Information			
25	User can verify the cardholder and management account information.	The EAS shall allow for the verification of account holder and management account information and the following fields: a) Employee identification, name, address, telephone, fax, email b) Approving official name, address, telephone, fax, email c) Supervisor name, address, telephone, fax, email d) A/OPC name, address, telephone, fax, email e) Designated Billing Office information f) Organizational roles g) Unit within agency/organization	34
Scenario 8: Modify Account Information for Agency/Organization Program Coordinator (A/OPC)			
26	A/OPC can modify an existing managing account.	The EAS shall allow for authorized users to add new account holder account numbers to an existing managing account or move account holder account numbers from one managing account to another.	35

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
27	A/OPC can modify information on an existing cardholder and managing account.	The EAS shall allow the A/OPC to modify the following information on an existing account holder and managing account a) Employee identification, name, address, telephone, fax, email b) Approving official name, address, telephone, fax, email c) Supervisor name, address, telephone, fax, email d) A/OPC name, address, telephone, fax, email e) Designated Billing Office information f) Organizational roles g) Unit within agency/organization	36
28	A/OPC can perform a bulk account information change	The EAS shall provide a capability to perform bulk account information changes.	37
Scenario 9: Access and Maintain Controls (bulk updates)			
29	EAS is able to verify and change dollar and transaction limits.	The EAS shall provide a mechanism to set and verify transaction limits for the following: a) Daily spend limit (e.g. cash) b) Cycle spend limit (e.g. cash) c) Transaction size limit d) Daily transaction limit e) Cycle transaction limit f) Limit government to government transaction size	17,38

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
30	EAS is able to verify and allow authorized users to change MCC and/or Product Number/Code restrictions.	The EAS shall allow authorized users to perform the following for MCC and/or Product Number/Code maintenance: a) Verify account MCC and/or Product Number/Code restrictions b) Block all MCCs and/or Product Number/Codes c) Unblock all MCCs and/or Product Number/Codes d) Block single MCC and/or Product Number/Code e) Unblock single MCC and/or Product Number/Code f) Develop preset MCC and/or Product Number/Code blocking template g) Set MCC and/or Product Number/Code blocking template to account Additionally, The EAS shall provide authorized users with the ability to change category block templates (e.g., blocking templates), purchase limits, and activation status. Finally, the EAS shall provide authorized users with the ability to limit value of large intra-governmental transactions (e.g., not allowing transactions greater than $100,000).	39, 40, 41
31	Authorized user can verify the account status for the accounts they manage.	The EAS shall provide a capability to allow for authorized users to verify account status for each assigned user account: a. New b. Approved c. Active d. Inactive e. Suspended f. Cancelled g. Open/Closed	42
Scenario 10: Account Activation and Deactivation			
32	Authorized users can activate accounts while performing bulk updates.	The EAS shall allow access for bulk account activations of one or more accounts at a time.	44

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
33	Authorized users can de-activate accounts while performing bulk updates.	The EAS shall provide automatic activation and deactivation of accounts on date specified by agency/organization. No transactions shall be authorized on a deactivated account. If an account is deactivated, customers assume no liability for transactions. Additionally, the EAS shall allow for access and control maintenance for bulk updates for account de-activations of one or more accounts at a time.	45, 46
34	Authorized users can close accounts while performing bulk updates.	Contractor shall show that the EAS can close out one or more accounts while using the Access and Controls bulk updates capability.	47
35	Comments can be added to individual EAS accounts.	The EAS shall provide authorized users with the ability to post comments to accounts (e.g., a detailed explanation for the reason the account was suspended).	43
Scenario 11: Perform Access Inquiries			
36	Authorized users can access the required online functionality to complete an account/cardholder application.	The EAS shall allow for users to complete online account/account holder application and ability to track application status and verify receipt or other user requests as identified at the agency / organization task order level.	48
37	Authorized users can access the required online functionality to view and use the Online Payment options.	The EAS shall allow authorized users online payment functionality and options for CBAs.	2,49
38	Authorized users can access the required online functionality to view and use the Online Invoice options.	The EAS shall provide options for authorized users to view and use online invoicing capabilities.	50

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
39	Account Inquiry -- Users can search by cardholder name(s)	The EAS shall allow authorized users to perform account inquiries through a combination of name, account number, and other account specific information.	51
40	Account Inquiry -- Users can search by account number(s)	The EAS shall allow authorized users to verify account information while performing account inquiries.	52
41	Account Inquiry -- Users can search for users with different roles within the EAS for their agency\organization	The EAS shall allow authorized users to verify managing account information while performing account inquiries. Additionally, the EAS shall allow authorized users to perform account inquiries through a combination of name, account number, and other account specific information. Finally, the EAS shall allow authorized users to verify account information while performing account inquiries.	51, 52, 53
42	Account Inquiry -- User is able to verify cardholder account information.	The EAS shall allow authorized users to verify account information while performing account inquiries.	52
43	Account Inquiry -- User is able to verify the managing account information.	The EAS shall allow authorized users to verify managing account information while performing account inquiries.es.	53
Scenario 12: Tracking Account Activities, Access and Changes			
44	While an authorized user is reviewing an account access history, the history will show when a Cardholder or A/OPC has accessed the account.	The EAS shall maintain an audit trail of account activity, updates, and user activity by card management personnel (e.g., primary vs. alternate A/OPC), as specified in C.8 Security Requirements. And, the EAS shall maintain in the account history an access log showing the times, dates, and actions of the user and A/OPC and make the history and logs available to authorized users.	54, 55

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
45	While an authorized user, a Cardholder or A/OPC, is reviewing an account and makes any changes to the account, the history will show when the account was accessed and a session history, and a record of all activities and changes that were made on the account.	The EAS shall maintain a log of all users who have accessed or made changes to an account and at a minimum, capture the following: a) When account was accessed b) Session history c) Record of all activities and changes made to account	56
46	EAS is capable of providing access reports for specified accounts.	The EAS shall be capable of producing customizable access log reports for one or more specified accounts, in an electronic format.	57
Scenario 13: Manage Convenience Checks			
47	EAS will allow for the Cardholder or A/OPC to manage the convenience checks and options for the account.	The EAS shall provide a mechanism for the account holder or A/OPC to manage the convenience checks and options for the account. a) A/OPC can overrule the option to allow for convenience checks to be added to the account b) A/OPC may cancel request for additional checks c) Account holder requests convenience checks be added to the account and order additional checks d) Account holder and A/OPC are able view all spent checks on the account and stop payment on any outstanding checks. Additionally, the EAS shall provide summary data for convenience checks to include check numbers and names of merchants.	59, 60
Scenario 14: Purchase Logs and Purchase Reports			

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
48	EAS shall provide a purchase card log functionality with the capability to run reports from the purchase log data.	The EAS shall provide a Purchase account log functionality with the capability to run reports from the Purchase log data (e.g., aggregated strategic source data).	58
Scenario 15: Transaction Maintenance Electronic Reconciliation			
49	Cardholder can verify transactions.	The EAS shall provide a capability to allow account holders to verify all transactions listed on online statements with invoice/posted transactions and that the transactions match and any discrepancies shall be easily identifiable.	17,61
50	Cardholder can verify transactions details.	The EAS shall provide a capability for account holders to verify that each transaction listed on the online statement and data for single transactions listed for online statements matches invoice/posted transactions. Additionally, the account holder is able to attach reconciliation notes/comments to individual transactions.	2,17,62
51	Cardholder is able to approve transactions.	The EAS shall provide a capability for approving and disputing individual transactions.	17,63

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
52	Approving Official (AO) is able to approve all reconciled transactions from the Cardholder.	The EAS shall provide authorized users with electronic review and manipulation of all captured transaction information to include the ability to: a) Support electronic reconciliation and certification of invoices b) Sort data by any field c) Filter out unnecessary information d) Edit account allocation manually, as needed e) Split transaction amounts into sub-units for multi-account allocation This includes summary roll-up, review, and manipulation at different levels and an account summary, including historical spend, delinquencies, month over month for a minimum of one year. An account snapshot shall include CBA credit limit fluctuations.	17,64
53	Transactions that are approved by an AO are made available for review from within the EAS.	The EAS shall provide a capability to approve all reconciled transactions from the account holder: a) AO is alerted after account holder has completed reconciling transactions b) AO is able to review each transaction and approve or reject individual transactions c) When AO approves transactions, the EAS submits reconciled transactions for approval	17,65
54	Rejected transactions are recorded, tracked, and available for the AO to review, un-certify, and notify account holders.	The EAS shall provide a capability to write and have associated notes/comments recorded, tracked, and available. AO is able to view rejected transactions and associated notes, un-certify the transaction, and notify account holders.	17,66
55	Cardholder or AO, or higher approver can match credits to purchases from within the EAS.	The EAS shall provide a capability to the Account holder, AO or higher authorized approver so they can match credits to purchases.	17,67
Scenario 16: Transaction Disputes			

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
56	Cardholder and A/OPC can dispute transactions from within the EAS.	The EAS shall provide a capability for the A/OPC to dispute transactions. a) Clearly displays when an account holder or A/OPC disputes a transaction. b) The EAS shall email both account holder and A/OPC notifying that a disputed transaction has been identified and is being processed. c) Account holder and A/OPC can view the status of a dispute, cancel a dispute at any time, and ensure an email is sent to the account holder and A/OPC when resolved or provide the capability to cancel a dispute if the dispute was resolved with the merchant.	68
Scenario 17: Viewing Account Statements, Transactions, and Master Accounting Codes			
57	Cardholder can access the EAS and view the current account statement online and perform inquires.	The EAS shall allow authorized users to access the EAS and view account statements and perform inquiries. a) View account statements b) Sort/filter transaction data using multiple data fields c) View itemized invoices associated with each statement entry d) The A/OPC can refine searches for specific account numbers and/or names Additionally, the EAS shall provide the ability to search and sort by a specific value in a line of accounting (e.g., searching and sorting by organization codes within a common line of accounting).	2,69, 72

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
58	Cardholder or their A/OPC can perform allocations for transactions using the master accounting codes and EAS can be used to set automatic defaults for automatic default cost allocations for each transaction .	The EAS shall provide authorized users with automatic default cost allocations for each transaction to include: a) Ability to assign an agency/organization account code automatically to each transaction as determined by the A/OPC b) Ability to assign a code based on the merchant, merchant category, account holder or any combination of these fields c) Account code shall be sufficiently long to accommodate the accounting string of any agency/organization (maximum 150 characters) Ability of the A/OPC to override the default code; agency/organization will specify multiple accounting codes at the task order level, as applicable The EAS shall allow the A/OPC to override the default accounting codes and assign accounting codes to transactions. Additionally, the EAS shall allow the user to allocate transactions with master accounting codes.	71, 73, 74
59	Cardholder can allocate transactions.	The EAS shall allow authorized users to allocate transactions across multiple lines of accounting and reallocate entire transactions to a new line of accounting.	75
Scenario 18: Reporting Capabilities			
60	EAS users can perform basic functions while viewing reports.	The EAS shall have the capability for reports to be downloaded into Microsoft Excel format, printed, and saved in a location specified by the user, emailed to the user, and saved in the EAS for future reference. Reports shall not include PII.	76

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
61	User can create and view ad-hoc reports.	The EAS shall, at a minimum, provide the capability for users to create ad-hoc reports, save reports, modify reports, export reports to MS Excel (.xls, .xlsx), .txt, .pdf, .csv or other formats specified by the agency/organization. Second verify that the EAS shall provide authorized users with the ability to flag and generate reports on transactions where state and local taxes have been assessed; and finally that the EAS shall provide user defined date ranges (e.g., quarterly, biannually, annually) for report generation.	77, 78, 79
62	User can view standard agency reports (For descriptions, see **C.7.3.1 Agency/Organization Reporting Requirements**)	The EAS shall provide authorized users with standard commercial reports, by business line, as specified in **C.7.3.1 Agency/Organization Reporting Requirements.**	78,79,80
63	EAS shall update program and transaction data (to include delinquency information) as listed in **C.7.2 Program and Transaction Data.**	The EAS shall update program and transaction data (to include delinquency information) as described in **C.7.2 Program and Transaction Data** to reflect all payments and transactions as of 11:59 p.m. EST on previous business day.	70
64	Users can view standard GSA Data Files.	The EAS shall provide the capability to integrate and view standard GSA Data Files (see **C.7.2.2 Program Data).** Note these reports are not a requirement of the EAS but will be validated as part of the LTD process. a) Government-wide Aging Analysis Data File b) Agency/Organization Refund Data File c) Socioeconomic Data File d) FedRooms Hotel Report	81

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
65	EAS has Single Sign On capability.	The EAS shall provide single sign-on capability if required by the agency/organization, in accordance with security requirements stated in **C.8 Security Requirements.** Updates to user passwords shall apply to all Contractor systems.	14
Scenario 19: Contractor Demonstrates			
66	Secure messaging is supported.	The EAS shall provide connectivity that facilitates electronic information sharing among agencies/organizations to include: a) Ability to allow multiple users concurrent access to the application and, if requested by the agency/organization b) Allows data through a local or wide area network (LAN/WAN) c) Ability to send email notification to cardholders of online statement availability Multiple connectivity options necessary to electronically link users using customer technology (options should include LAN, WAN, client/server, internet, and e-mail)	83
67	EAS is complaint with C.8 Security Requirements.	The EAS shall provide the capability to ensure all program and transaction data is secured, at a minimum according to C.8 Security Requirements.	82

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
68	EAS provides various connectivity methods to facilitate electronic information sharing among agencies / organizations.	The EAS shall provide authorized users with the ability to download data from the system. This includes the automatic creation and daily transmission of files containing accounting data (via secure electronic transfer) to agency/organization internal accounting systems. The Contractor shall provide program and transaction data in a format and frequency specified at the task order level (**C.7 Data Management, Transaction Support and Reporting).** If requested by the agency/organization, this shall include a custom interface file to any internal system(s) designated by the agency/organization. This custom interface file shall be created in such a manner that it can be imported into the agency's/organization's system with no interaction, special programming, or manual entry of transaction data. • The Contractor shall also have the capability to compress custom interface files into zip files • The Contractor shall make adjustments or updates to the agency/organization interface as required by the agency/organization for revisions to agency systems, migration to new agency systems, and/or if the agency/organization contracts with a government shared service center for financial management services and provide authorized users with the ability to discern how a transaction is completed (e.g., point-of-sale, Internet), if passed by the merchant;	84

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
69	EAS is tested and certified for conformance with Section 508.	GSA reserves the right to access the Contractor's EAS in order to review the system for 508 compliance conform at any time. The EAS shall be recertified after each release (e.g., minor, major, or patch). The EAS is not required to conform with Section 508 prior to award. As such, this step will not be rated. For further guidance see C.2.2 Transition and H.12.9 Ordering Process.	86
70	EAS shall be available at all times, 24 hours a day, every day of the year.	The EAS shall be available 24 hours a day, every day of the year, except in the case of routine maintenance and periodic upgrades for which the Contractor shall give a minimum of 30 calendar days' notice prior to the event. The Contractor shall notify the agency/organization about hardware/software patches done on an emergency basis to remove security vulnerabilities..	85
Scenario 20: Card Type Identifier			

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
71	Purchase and Travel card holders are uniquely identified through a system generated customer number to protect the Cardholder identity and card numbers.	The EAS shall require a unique identifier for every Purchase and Travel accountholder. a) The unique identifier should be system generated with a combination of alpha/numeric letters b) The unique identifier could be linked to the account or account holder SSN. This allows for account identification other than using any part of the account holder account number c) The agency would determine the convention (e.g., Purchase cards start with "P", Travel cards with "T" for identification, Integrated cards with “I”)	88
72	Purchase and Travel card Cardholders have a .gov email address linked to their account at all times.	The EAS shall require an email address consistent or associated with the customer agency/organization, included but not limited to: .gov, .mil, .edu, for all account holders and approving officials, in addition to personal email addresses. The EAS shall prompt user (account holder and non account holders), to verify accuracy of e-mail addresses (in addition to other personal contact info), within 180 calendar days.	89
73	Authorized user may download all of the email addresses linked to one or more specified cardholders, including the AO.	The EAS shall allow authorized users the ability to download all email addresses in the account holder account, including the AO.	90
74	EAS capabilities exist for authorized users to message the Cardholders.	The EAS shall provide the ability to send messages to cardholders from the bank system.	91
Scenario 21: GSA EAS Access			

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
75	EAS includes the Fraud Analytic capabilities described in the Master Contract.	The EAS shall be accessible to authorized GSA users at an aggregate government-wide level to run fraud analytic tools, perform inquires, view trends, view/update dashboards, run reports, and have the ability to export data.	93
Scenario 22: MAC Operating System			
76	User is able access the system using a MAC device.	The EAS shall be able to adapt to meet additional future requirements due to program volume growth and technological advances, as stated in **C.2.2.1.3 Technological Advance Transition,** at the Contractor's expense.	87, 92
Scenario 23: Adding Comments to Reports			
77	When comments are added to a ad-hoc or canned report, the comments appear intact.	The EAS shall enable all comment(s) fields to be included in ad-hoc or canned reports and/or extracted when requested.	94
Scenario 24: Account Management Views			
78	All attributes for closed accounts remain intact.	The EAS shall retain all account data and attributes for all closed accounts, maintain all transactional data including accounts with no transactions, and make the data available for inclusion in reports (ad-hoc or canned).	95

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
79	FM, FO, AOPC has view-only access to the screens for the cardholders over which they manage.	The EAS shall have a Cardholder View only access for the Financial Manager (FM), Financial Officer (FO), A/OPC for the cardholders over which they manage.	96
Scenario 25: Attachments and Supporting Account Documentation			
80	Attachments can be uploaded for transactions.	The EAS shall allow the Cardholders to have the ability to upload supporting documentation (attachments) for each transaction in their statements at any time.	97
81	Supporting documentation can be downloaded by authorized users.	The EAS shall allow all supporting documentation or statement attachments to be downloaded by the AOs, AOPCs, FMs for each of the Cardholders they manage.	98
82	Supporting documentation is retained for the specified retention period.	The EAS shall maintain all supporting documentation or attachments to statements that were attached by cardholders in alignment with **C.7.2.4 Record Retention and Retrieval,** unless otherwise specified by the agency/organization. for an indefinite period of time (or as defined by the Agency).	99
83	EAS has discretionary fields for custom data.	The EAS shall have a minimum of eight (3 designated for Travel only) five discretionary fields designated for customized data population.	100

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
Scenario 26: Account Maintenance History			
84	Maintenance History events are captured when maintenance events occur.	The EAS maintains all Maintenance History including all maintenance events regardless of the source, to include maintenance: 1) performed by the Contractor 2) performed by the Agency and 3) performed through a Bulk Maintenance upload by the Agency and the history will show the date, who performed the maintenance, and the changes that were made to the system and/or data.	101
85	Maintenance History log retention is set for 15 months.	The EAS maintains the Maintenance History log and makes the log available to download into a report extract or query, and retain the Maintenance History for a rolling 180 months (15 years).	102
Scenario 27: ATM Limits and Authorizations			
86	EAS can set ATM limits and other temporary account settings.	The EAS shall allow authorized account managers to apply temporary changes to a Cardholder account they manage including adding Begin Date and End Date fields, for such activity as MCC templates, single transaction and card limits, ATM cash percentages/amounts.	103
87	Comments History field is available and maintained.	The EAS shall maintain the Comments Field history and keep the history intact with an account (see **C.7.2.4 Record Retention and Retrieval**), even when a replacement card is issued or an account is closed.	104
88	ATM cash limits is maintained for each account.	The EAS shall have an ATM cash percentages/amounts amount field and allow for each AOs, AOPCs, and FMs to modify this field for each of the Cardholders they manage.	105

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
89	Changes to a Cardholders ATM Cash percentages are made real-time.	The EAS shall update the effected Cardholders ATM cash percentages/amounts settings as soon as the AOs, AOPCs, FMs make changes to the field.	106
Scenario 28: Administrative Account and Bulk Maintenance			
90	EAS allows Agencies the capability to create administrative accounts.	The EAS shall provide the capability for the Agencies to create administrative user accounts (e.g., A/OPC's, Financial Analysts, etc.).	107
91	EAS provides the ability for the Agencies to upload BULK MAINTENANCE Excel files for all types of account changes to include, but not limited to, card limits, mass hierarchy realignments, MCC and/or Product Number/Code Templates, credit worthiness codes, discretionary code fields, and apply the changes to the accounts in the EAS.	The EAS shall provide the ability for the Agencies to upload BULK MAINTENANCE Excel files for all types of account changes to include, but not limited to, card limits, mass hierarchy realignments, MCC Templates, creditworthiness codes, discretionary code fields, and apply the changes to the accounts in the EAS..	108
92	EAS provides BULK MAINTENANCE upload capabilities to include the ability to assign a Begin Date and End Date for temporary changes to card limits, single transaction limits, ATM cash percentage, MCC and/or Product Number/Code templates, etc.	The EAS shall provide BULK MAINTENANCE upload capabilities to include the ability to assign a Begin Date and End Date for temporary changes to card limits, single transaction limits, ATM cash percentage, MCC and/or Product Number/Code templates, etc.	109
93	EAS Bulk Maintenance upload feature does not have limits to the number of records being uploaded in each session.	The EAS BULK MAINTENANCE upload feature shall update all records uploaded in each upload with no limitations on the number of records in each session.	110

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
94	EAS has a BULK MAINTENANCE upload in a Comments Field and retain the comments in the Maintenance History Log.	The EAS shall allow for comments to be added for each BULK MAINTENANCE upload in a Comments Field and retain the comments in the Maintenance History Log and the Log should be able to be retrieved for most recent six (6) years with the remaining full log from the full period of performance available by other means (tape storage, etc.).	111
Scenario 29: AOPC Alerts and Notifications			
95	AOPCs can designate required alert and email alert settings including an alert about auto close to be used, set reminders to verify contact information, phone and email address, etc..	The EAS provides the ability for AOPCs to designate required alert and email alert settings including an alert about auto close to be used, set reminders to verify contact information, phone and email address, etc..	112
Scenario 30: Fields and Labels			
96	EAS shows all field labels.	The EAS shall have labeled fields so that the purpose is clear to users.	113
97	Flyover text functionality is shown by placing the mouse pointer or focus on a field title.	The EAS shall have flyover text on each field to display the full field name, hints or help for the user, and a link to system help and glossary.	114
Scenario 31: Accounting, Transaction Approvals, MCC and/or Product Number/Code, Service Providers Templates and Logs			

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
98	Accounting is attached to all statements prior to approval.	The EAS shall verify that when AOs and Cardholders submit and approve statement accounting is attached and if no accounting is attached an error message is displayed and the EAS does not allow for it to be submitted.	115
99	EAS validates each transaction prior to approval and transmission.	The EAS shall require all transactions to have proper accounting before they are approved and transmitted.	116
100	AO can reallocate statements.	The EAS shall allow the AO full control to reallocate statements until they are closed or auto-closed.	117
101	MCC and/or Product Number/Code functionality provides for a Vendor template, vendor MCC and/or Product Number/Code blocking, variable MCC and/or Product Number/Code attributes, and name display.	The EAS shall provide the following functionality to support MCC codes: • Ability to establish an MCC and/or Product Number/Code template by Vendor Name, not Vendor MCC. • Ability to block a specific vendor from an MCC and/or Product Number/Code • Ability to limit the attributes of a single (or multiple) MCC and/or Product Number/Code within an MCC and/or Product Number/Code Template, including daily limits, cycle limits, # transactions, etc. • Display all given and pseudonym names.	118
102	EAS supports Level 4 hierarchy numbers.	The EAS shall support an unlimited amount of Level Four (4) hierarchy numbers.	119
103	Transaction data is sent to the Agency.	The EAS shall send daily transactions to the Agency the day after transactions post with all account file data.	120
104	Validation check is in place for all vendors transactions.	The EAS shall validate that all vendors supply itemized details for all items purchased in each transaction, Level Three (3) data must be populated (as available).	121

GSA SmartPay3 Live Test Demonstrations

Critical Functions Test Scenarios

Step	Step Description / User Action	Expected Results	Requirement
105	EAS provides service provider templates.	The EAS shall provide templates for service providers to allow for standardized and timely setup of FMs, Foes and other designated agency personnel when employees change.	122, 123
106	Purchase card log functionality must track the status of purchases.	The EAS shall provide a purchase card log attached to each statement within the EAS and allow cardholders could update tracking purchases and checking off when they post and show the AO who authorized the purchase and date of authorization. The EAS shall enable accountholders to attach documents to statements or transactions, as outlined in the requirements at the agency/organization task order level.	124
End of Demonstration			