Connect Security

Tech Note

Important

The below information encompasses the entirety of the Connect security capability and includes features as provided by PrivaWall (more information in the PrivaWall tech note) within Connect to apply to email rule based operations.

It should be noted that not all features of PrivaWall are exposed from within Connect's dashboard and configuration. In particular, Content Filtering. DLP (Data Leak Prevention) and Intelligent Email Relaying). Should these capabilities be required they may be configured separately by Pitney Bowes.

v2.0 - December 2017

Overview

The Connect contains a range of state of the art security technology (Privawall and PostalGuard) to cover all aspects of Authentication, Email Encryption, Antispoofing and Antispam measures, for secure interfacing to a customer's online services transactions systems.

Connect Security

EMAIL SECURITY

The Connect system implements a wide range of technologies to authentication both the customer(ActiveProvider) side and the user for email authentication in sending and reading of emails.

ONLINE CUSTOMER LOGIN BASED AUTHENTICATION

Connect leverages existing online customer authentication methods by forwarding authentication credentials to the existing authentication infrastructure (by means of a web service/http communication). Users' passwords are not stored on Connect servers. Upon successful authentication, the security token (if returned) can later be used for performing transaction.

SYMMETRIC AUTHENTICATION

Connect's symmetric authentication employing a dedicated password for reading e-mails. The password is stored encrypted on Connect servers and managed by the bank using web services enabling easy password management via the online customer UI.

AUTOMATIC AUTHENTICATION

Connect's automatic authentication is a dedicated, unique, randomly generated token stored on the users' machine (akin to SoftToken) in order to identify the user when composing messages. The customer can decide whether this form of authentication is sufficient according to the performed action, if a more challenging authentication method is needed, then the system can trigger a higher level of authentication

EMAIL SIGNING

Email sent through the Connect servers can be digitally signed according to the S/MIME protocol.

The system supports corporate signature and/orprivate signature. In order to sign corporate emails, since the original From mail address differs from the signing signature, PostalGuard is able to replace the From address to match the signing certificate, while leaving the reply address intact, without breaking the signature and validity of the S/MIME certificate. The sender's digital signature is placed in a digital certificate, and this certificate is attached to every email that the sender sends. Properly implemented digital signatures are equivalent to traditional handwritten signatures in many respects, but are more difficult to forge than the handwritten type.

The PostalGuard security solution uses a standard S/MIME (Secure / Multipurpose Internet Mail Extensions) certificate to S/MIME sign all email messages, original mail, archive copies, and corporate emails that pass through it. When the recipient receives the email, the email client of the recipient checks that the digital certificate belongs to the sender, and that the certificate is still valid. Any

standard email client, such as Outlook, Outlook Express, Lotus Notes, Thunderbird, and more, can perform this operation.

This standard is supported across virtually all mail clients but its support in webmail environments is lacking. In addition, a digital signature can also be created within the encrypted block to verify its authenticity when using webmail solutions.

EMAIL ENCRYPTION

Connect email content is encrypted using the standard AES algorithm with 256 bit key length.
When using guaranteed delivery or when using online customer authentication for reading messages, a unique one time encryption key is used and is stored at the bank. Only after successful user authentication that key is retrieved and sent to the user machine to perform the message decryption. Encrypted content may also include embedded attachment data or alternatively can point to attachments stored (encrypted) on the customer's servers.

CERTIFIED DELIVERY

As part of the Connect encryption process, the message can be encrypted using a unique one time key that is stored at the customer's servers. Only after the user authenticates, that key is sent to the user machine and the message can be decrypted, thereby notifying the server that the user has opened the specific message.

TRANSACTIONS AND ONLINE CONTENT SECURITY

Securing transactions – SSL, Additional optional based on the action type …. Authentication process based on the online customer authentication or the symmetric authentication…

RULE BASED POLICY ENGINE

PRIVAWALL POLICY ENFORCEMENT (the 'Engine')

The PrivaWall Policy Enforcer provides real-time management of policy decisions for each and every e-mail message routed to PrivaWall. The decisions are made using the rules stored in the PrivaWall Rule Base. These rules specify the actions to be enforced on each message according to its content, its owners and other specifications.

Rules may be enforced to an e-mail message according to its sender and/or recipient, according to its contents and according to its attachments. Once the rules that apply to the specific e-mail are determined, the e-mail is processed according to the pre-defined actions relating to those rules. Primary actions include:

- Encryption (The rule also indicates which encryption method should be applied and which encryption key to use)
- Preventing the sending of the message
- Message logging and/or archiving
- Adding of specific notes

- Requesting of a receipt
- 'Parking' of an e-mail till a specific action takes place
- Routing the message to various destinations
- Adding or removing recipients
- Taking no action

Rule-Based Policy Definition and Enforcement

PrivaWall's rule-based logic and keys/certificate management enables the system administrator to selectively determine which actions to perform. Rules are simple to formulate and enter. The following features are made possible by the rule based policy:

1. Rules can be added, edited and deleted independently of each other
2. Applying changes to the rules does not require PrivaWall to be shut down
3. Any list of clients can be served by the system – PrivaWall does not have
4. to serve all the users of the corporation
5. The privacy of users in their personal or private correspondence is respected
6. Rules can be copied from one policy to another

Rule Management

A key feature of PrivaWall is *rule management*. The security administrator has an intuitive tool for expressing e-mail security policy. The rules are structured into two parts:

1. The 'If' part, or condition, specifies the condition for which a rule applies
2. The 'Then' part, or action, specifies the action to be taken with the message if the rule applies

The actions that may be taken are divided into two groups

- Main Action - Hands off, Fail to all, Fail to catch recipient, Encrypt, 'Park', 'Park All Messages', Erase Message and Not set.
- Additional Actions:
    - Log message
    - Archive
    - Return Receipt, Add notes
    - Add or Remove recipients, Strip HTML, S/Mime Signature, Send Plain Text
    - Copy, Remove caught attachment, Alternate SMTP Routing, Set 'Reply To' field.

Incoming Email - Content Filtering

Anti-Virus Scanning

Over 90% of viruses arrive via detachable media connected to the workstation. Increased connectivity has enabled viruses to spread rapidly causing more destruction than ever before.

With the Built-In Anti-Virus product integrated in PrivaWall, Anti-Virus protection is easy, fast and reliable. PrivaWall provides access to a built in anti virus scanning engine technology. The scanning

engine is accessible from within the PrivaWall system. This unique architecture optimizes the resource use of different scanning engines (e.g. minimizing file access by sharing files with all scanning engines). This Anti-Virus is renowned for its unsurpassed malicious code detection and disinfection capabilities through the use of multiple best-of-breed scanning engines, and its high performance through resource optimization.

File Type Analysis for White List Policy

Attachments both in incoming and in outgoing mail can be analyzed according to the file extension. This analysis is performed on the internal structure in order to ensure that the structure fits the file description defined by the extension. PrivaWall is able to analyze the structure of the following 65 file types:

1. aif
2. aiff
3. zip
4. rar
5. rtf
6. pdf
7. wri
8. qtif
9. mpa
10. Ocx
11. com
12. vxd
13. avi
14. mp3
15. qif
16. mpd
17. dot
18. xla
19. au
20. midi
21. wmf
22. mpx
23. qt
24. xlt
25. mdb
26. mde
27. pst
28. mov
29. moov
30. mpt
31. cab
32. jpe
33. scr
34. vss
35. vsd

36. vst
37. mpp
38. bmp
39. gif
40. jpg
41. jpeg
42. wma
43. msg
44. cry
45. wpd
46. exe
47. sys
48. dll
49. class
50. asf
51. ram
52. asf
53. mpeg
54. mpg
55. mpe
56. pot
57. arj
58. ra
59. doc
60. xls
61. ppt
62. wav
63. mid
64. wmv
65. pps

Unwrapping objects embedded in Office documents

PrivaWall can check inside Office documents for embedded objects, scans these for viruses and can apply rules to them. Consequently, by embedding an EXE file within a Word document will not prevent it being virus scanned or bypass a rule that prevents EXE files from being sent into the organization.

Blocking of Macros

PrivaWall can be set to block Macros embedded in Office documents.
If the document contains a macro, fail the message' option should be selected (check marked) if PrivaWall is to fail the message if it contains an Office document (Word, Excel) or an MS Project that contains a macro. This is useful because most new viruses come in form of a macro.

Note: PrivaWall does not detect if a PowerPoint or a Visio document contains a macro.

Stripping of MIME types

A set of MIME types can be defined that PrivaWall will strip from incoming and/or outgoing messages. This method can, for example, strip the 'text/html' part of a message, which can potentially contain a malicious script.

Stripping of suspected 'Reply-To' headers

PrivaWall has an option to strip the 'Reply-To' headers from messages and to add an entry to the log if the 'Reply-to' address does not match the message 'from' address.
The 'Reply-To' header is used when the user clicks the 'Send Back' action in his/her mail client to create a new message with the address in the 'Reply-to' header as a recipient. This option can also be used maliciously, to trick the recipient to replying to a different address.

Block protected Office, PDF and Zip archives

There is now an option to block Zip files containing protected files that cannot be scanned for viruses. The 'If can't unzip, fail the message' option should be selected (check marked) if PrivaWall is to fail the message when it is unable to unzip some (or all) of the attachments.

An automated message can be sent to the sender if PrivaWall fails the message.

Note: The notification will be sent only if the 'Notify sender' option has been selected.

Outgoing Email - Content Filtering

Text Content Filters

PrivaWall can check and analyze files according to their contents using the capabilities of a unique content filtering Engine.

The file contents can be searched for predefined expressions and if found, can trigger specific actions. Expressions can be either in the form of a Boolean expression (cat and dog) or as a category. This feature is especially useful for catching sensitive information as it is being brought in to the network.

PrivaWall supports a number of search request types. A natural language search is any sequence of text, like a sentence or a question. After a natural language search, PrivaWall sorts retrieved documents by their relevance to your search request.

A Boolean search request consists of a group of words or phrases linked by connectors such as 'and' and 'or' that indicate the relationship between them.

NATURAL LANGUAGE SEARCH

A natural language search request is any combination of words, phrases, or sentences. After a natural language search, PrivaWall sorts retrieved documents by their relevance to your search request. Weighting of retrieved documents takes into account:

- the number of documents each word in your search request appears in (the more documents
- a word appears in, the less useful it is in distinguishing relevant from irrelevant documents);
- the number of times each word is found if the request appears in the documents
- the density of hits in each document.
- Noise words and search connectors like NOT and OR are ignored.

Synonym Search

Synonym searching finds synonyms of a word in a search request. For example, a search for fast would also find quick. You can enable synonym searching for all words in a request or you can enable synonym searching selectively by adding the '&' character after certain words in a request. Example: fast& w/5 search.

The effect of a synonym search depends on the type of synonym expansion requested on the search form. PrivaWall can expand synonyms using only user-defined synonym sets, using synonyms from PrivaWall's built-in thesaurus, or using synonyms and related words (such as antonyms, related categories, etc.) from PrivaWall's built-in thesaurus.

FUZZY SEARCH

Fuzzy searching will find a word even if it is misspelled. For example, a fuzzy search for apple will find appple. Fuzzy searching can be useful when you are searching text that may contain typographical errors, or for text that has been scanned using optical character recognition (OCR).
There are two ways to add fuzziness to searches:

1. Checking the "Fuzzy searching" box to will enable fuzziness for all of the words in your search request. You can adjust the level of fuzziness from 1 to 10.
2. Selectively using the % character. The number of % characters you add determines the number of differences PrivaWall will ignore when searching for a word. The position of the % characters determines how many letters at the start of the word have to match exactly.

Examples:

- ba%nana Word must begin with ba and have at most one difference between it and banana.
- b%%anana Word must begin with b and have at most two differences between it and banana.

PHONETIC SEARCH

Phonetic searching looks for a word that sounds like the word you are searching for and begins with the same letter. For example, a phonic search for Smith will also find Smithe and Smythe.

To ask PrivaWall to search for a word phonetically, put a # in front of the word in your search request. Examples: #smith, #Johnson

You can also check the Phonetic searching box in the search form to enable phonic searching for all words in your search request. Phonetic searching is somewhat slower than other types of searching and tends to make searches over-inclusive, so it is usually better to use the # symbol to do phonic searches selectively.

STEMMING

Stemming extends a search to cover grammatical variations on a word. For example, a search for fish would also find fishing. A search for applied would also find applying, applies, and apply.
There are two ways to add stemming to your searches:

1. Check the Stemming box in the search form to enable stemming for all of the words in your search request.
2. If you want to add stemming selectively, add a ~ at the end of words that you want stemmed in a search.

Example:

- Apply ~ Stemming does not slow searches noticeably and is almost always helpful in making sure you find what you want.

VARIABLE TERM WEIGHING

When PrivaWall sorts search results after a search, by default all words in a request count equally in counting hits. However, you can change this by specifying the relative weights for each term in your search request, like this:

apple:5 and pear:1

This request would retrieve the same documents as apple and pear but, PrivaWall would weight apple five times as heavily as pear when sorting the results.

In a natural language search, PrivaWall automatically weights terms based on an analysis of their distribution in your documents. If you provide specific term weights in a natural language search, these weights will override the weights PrivaWall would otherwise assign.

AND CONNECTOR

Use the AND connector in a search request to connect two expressions, both of which must be found in any document retrieved.

For example:

- apple pie and poached pear would retrieve any document that contained both phrases.
- (apple or banana) and (pear w/5 grape) would retrieve any document that (1) contained either apple
- OR banana, AND (2) contained pear within 5 words of grape.

OR CONNECTOR

Use the OR connector in a search request to connect two expressions, at least one of which must be found in any document retrieved. For example, apple pie or poached pear would retrieve any document that contained apple pie, poached pear, or both.

W/N CONNECTOR

Use the W/N connector in a search request to specify that one word or phrase must occur within N words of the other. For example, apple w/5 pear would retrieve any document that contained apple within 5 words of pear. The following are examples of search requests using W/N:

- (apple or pear) w/5 banana
- (apple w/5 banana) w/10 pear
- (apple and banana) w/10 pear

Some types of complex expressions using the W/N connector will produce ambiguous results and

should not be used. The following are examples of ambiguous search requests:

- (apple and banana) w/10 (pear and grape)
- (apple w/10 banana) w/10 (pear and grape)

In general, at least one of the two expressions connected by W/N must be a single word or phrase or a group of words and phrases connected by OR. Example:

- (apple and banana) w/10 (pear or grape)
- (apple and banana) w/10 orange tree

PrivaWall uses two built in search words to mark the beginning and end of a file: xfirstword and xlastword. The terms are useful if you want to limit a search to the beginning or end of a file. For example, apple w/10 xlastword would search for apple within 10 words of the end of a document.

NOT AND NOT W/N

Use NOT in front of any search expression to reverse its meaning. This allows you to exclude documents from a search. Example:

- apple sauce and not pear

NOT standing alone can be the start of a search request. For example, not pear would retrieve all documents that did not contain pear.

If NOT is not the first connector in a request, you need to use either AND or OR with NOT:
apple or not pear not (apple w/5 pear)

The NOT W/ ("not within") operator allows you to search for a word or phrase not in association with another word or phrase. Example:

- apple not w/20 pear

Unlike the W/ operator, NOT W/ is not symmetrical. That is, apple not w/20 pear is not the same as pear not w/20 apple. In the apple not w/20 pear request, PrivaWall searches for apple and excludes cases where apple is too close to pear. In the pear not w/20 apple request, PrivaWall searches for pear and excludes cases where pear is too close to apple.

NUMERIC RANGE SEARCH

A numeric range search is a search for any numbers that fall within a range. To add a numeric range component to a search request, enter the upper and lower bounds of the search separated by ~~ like this:

- apple w/5 12~~17

This request would find any document containing apple within 5 words of a number between 12 and 17.

Numeric range searches only work with positive integers. A numeric range search includes the upper and lower bounds (so 12 and 17 would be retrieved in the above example).
For purposes of numeric range searching, decimal points and commas are treated as spaces and minus signs are ignored. For example,

- -123,456.78

Would be interpreted as: 123 456 78 (threenumbers). Using alphabet customisation, the interpretation of punctuation characters can be changed. For example, if you change the comma and period from space to ignore, then 123,456.78 would be interpreted as 12345678.

Conditions

The 'Conditions' text filter allows you to define words/expressions for PrivaWall to 'Catch' in a scanned e-mail and then apply a rule on that specific e-mail.

PrivaWall allows you to use an 'Expansion Search' (Option for automatically expanding the search condition to include other grammatical forms of the given words such as adding 's' for plural, 'ing' etc) as well as 'Synonym Search' (Option for automatically expanding the search condition to include synonyms to the given words. For example, when searching for the word 'door' the search condition will be expanded to 'door' or 'portal' or 'entry')

Example:

- We can ask PrivaWall for a condition that says - Catch any outgoing e-mail that contains sensitive internal information, for example: 'Project C-130' and block that e-mail, return the e-mail back to the sender notifying him that he was trying to send sensitive internal information and at the same time report to the Security Manager.

Important notes:

- Using the 'Synonym Search' and especially the 'Use related words' feature can dramatically affect the time it takes PrivaWall to check whether the given condition applies to a message.
    - Clicking the 'Search Thesaurus' button activates the Thesaurus browse and shows how the search condition will be expanded. It is advisable to expand the condition oneself (i.e. not automatically) by looking at the synonyms and to avoid using the 'Synonym Search' and 'Use related words' directly.
    -

CATEGORIES

The 'Categories' text filter allows you to define sets of words related to a defined subject, for example: You can set all words/Expressions that you consider as related to spam and score each word with points and later ask that if the total score gathered on an e-mail exceeds the total score limit you have predefined, then apply a rule on that e-mail.

Example:

Let's define the following words to be considered as spam category table:

- Score: 30 Words / Phrases: XXX
- Score: 20 Words / Phrases: Viagra
- Score: 5 Words / Phrases: $
- Score: 20 Words / Phrases: Best deal
- Score: 5 Words / Phrases Lowest Prices

Now let's ask PrivaWall to consider an e-mail as related to Spam while it is being scanned only if it

- exceeds the score of at least 30 and reject such an Incoming e-mail.
- As PrivaWall scans our Incoming e-mail messages and finds an e-mail that contains the

- expression of: ‘XXX’ or maybe it found the following words: ‘Viagra’ + ‘$’ + ‘Lowest Prices’ –
- well, in that case the e-mail is considered as Spam and will immediately be blocked.

CONTENT FILTERING AND DATA LEAKAGE PREVENTION

The PostalGuard security solution prevents leakage of sensitive data, such as a combination of account details and sensitive information. It scans the content of the emails to identify potential leakage of sensitive data using its own text content filters that use the capabilities of a unique content filtering engine to check and analyze files according to their contents.

These filters catch any outgoing emails that contain sensitive internal information, block those emails, and then handle the emails according to the bank’s policy; they can be rerouted, returned to the sender with a notification that the email was not sent due to its sensitive internal information, create an email alert, create a copy to the relevant security officer, and more.

The PostalGuard Security Solution has two types of text content filters:

1. **Conditions text filter**
    a. Allows you to define words or Boolean expressions for PostalGuard to ‘catch’ in a scanned email.
2. **Category text filter**
    a. Allows you to define sets of words related to a defined subject.

CONDITIONS TEXT FILTER

The Conditions text filter allows you to define words or Boolean expressions for PostalGuard to ‘catch’ in a scanned email, and to then apply a rule on that specific email, such as returning to sender, notifying security manager, and more.

In addition to Boolean expressions, the solution supports the following additional conditions:

1. **Expansion search, Stemming**
    a. Automatically searches for grammatical variations of the words given in the search request, such as an added ‘s’ for plural, ‘ing’, and more.
2. **Synonym search**
    a. Automatically searches for synonyms of the words given in the search request.
3. **Fuzzy search**
    a. Finds words that have similar spelling to the words in the search request, even if they are misspelled.
4. **Phonetic search**
    a. Looks for a word that sounds like the word that you are searching for provided that it begins with the same letter.
5. **Numeric Range search**
    a. Searches for any numbers that fall within a range.

CATEGORY TEXT FILTER

The Category text filter allows you to define sets of words related to a defined subject. For example, you can set all words/expressions that you consider as related

to spam (the category), and score each word with points. Later you can request from PostalGuard to apply a rule on any email that has gathered a total score which exceeds the total score limit that you have predefined.

Variable Term Weighing

A Natural Language search is any combination of words, phrases, or sentences. After a Natural Language search, PostalGuard's solution sorts the retrieved documents by their relevance to your search request. Weighting of retrieved documents takes into account the number of documents each word in your search request appears in, the number of times each word is found, and the density of hits in each document. Following a search, PostalGuard's solution sorts search results. By default, all words in a request count equally in counting hits.

However, PostalGuard provides the option of Variable Term Weighing. Using this option, you can specify the relative weights of each term in your search request.

Harmful Inbound Email Prevention

Over 90% of viruses arrive via detachable media connected to the workstation. Increased connectivity has enabled viruses to spread rapidly causing more destruction than ever before.

PostalGuard provides access to a built-in antivirus scanning engine technology which is accessible from within the PostalGuard system. This unique architecture optimizes the resource use of different scanning engines (e.g. minimizing file access by sharing files with all scanning engines).

This antivirus is renowned for its unsurpassed malicious code detection and disinfection capabilities through the use of multiple best-of-breed scanning engines, and its high performance through resource optimization. With the built-in antivirus product integrated in PostalGuard, antivirus protection is easy, fast, and reliable.

Scanning of incoming emails for viruses includes the following processes:

1. **Analyzing file types of attachments**
    a. PostalGuard's solution analyzes attachments in incoming emails according to their file extensions. An analysis on the internal structure of the file is performed to ensure that the structure fits the file description defined by the extension.
2. **Unwrapping objects embedded in Office documents**
    a. PostalGuard's solution checks inside Office documents for embedded objects, scans these for viruses, and applies rules to them. Consequently, embedding a file within a document does not prevent it from being virus scanned.
3. **Blocking macros**
    a. PostalGuard's solution can be set to block macros that are embedded in Office documents.
4. **Blocking protected Office, PDF, and Zip archives**

    a. PostalGuard's solution blocks Zip files containing protected files that cannot be scanned for viruses.
5. **Stripping of MIME types**
    a. PostalGuard's solution strips incoming and/or outgoing messages that are of one of the predefined sets of MIME types. This method can, for example, strip the 'text/html' part of a message, which can potentially contain malicious script.
6. **Stripping of suspected 'Reply-To' headers**
    a. PostalGuard's solution can strip the 'Reply-To' headers from messages and can add an entry to the log if the 'Reply-to' address does not match the message 'From' address. The 'Reply-To' header is used when the user clicks the 'Send Back' action in his/her mail client to create a new message with the address in the 'Reply-to' header as a recipient. This option can also be used maliciously, to trick the recipient into replying to a different address Spoofing and Phishing Prevention

INBOX BRANDING

Connect email messages each receive a unique identifier which is pre-fixed to the message subject. And is stored at the bank database The Connect add-on queries the bank server with the message details including the recipient address and the subject. The server searches the database for a match and if one is found sends a confirmation back to the client. After the confirmation is received, the bank logo image is placed next to the 'From' field of the message and the 'From' field is optionally colored according to the bank theme.

Note:
This feature contains patent pending technology

DOMAIN KEYS

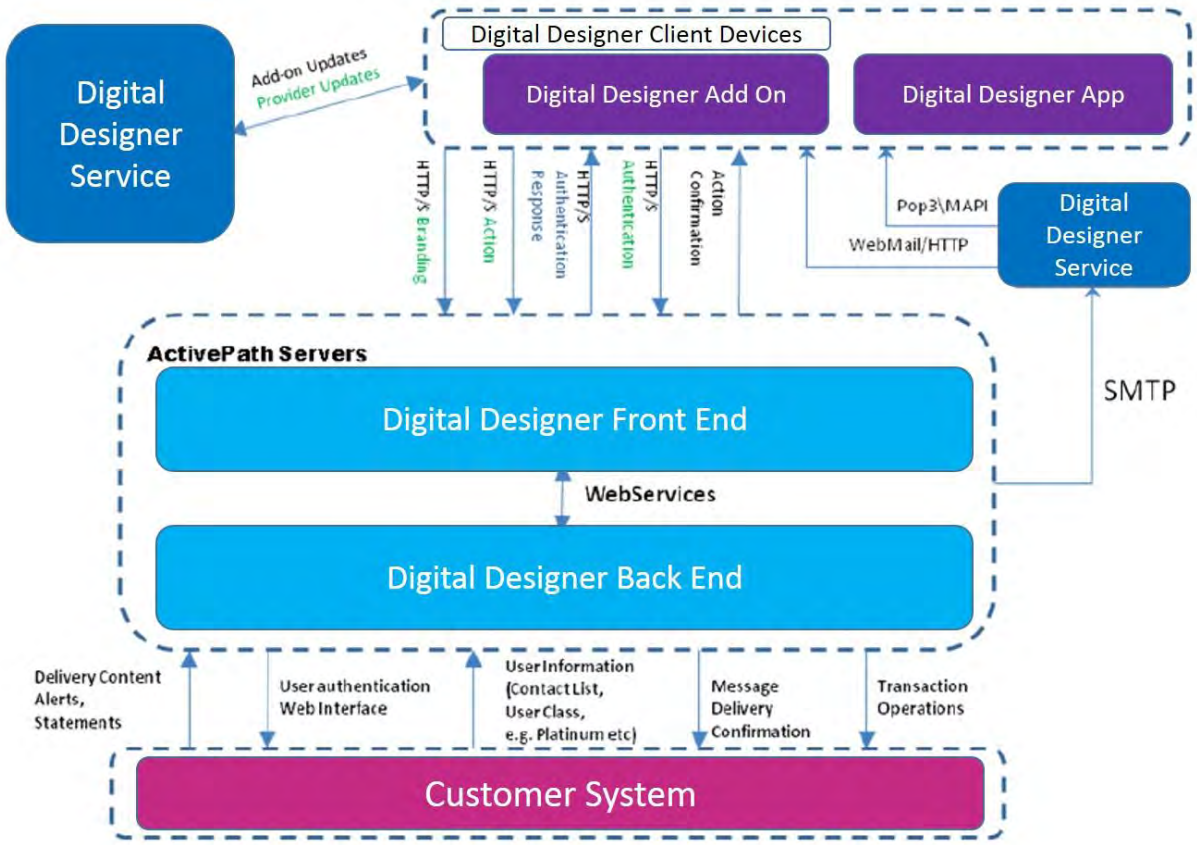
Email sent through the Connect servers can be signed according to the DomainKeys protocol (specified in RFC 4870) to reduce the chance of accidently tagging the messages as spam by antispam mechanisms.
Note:
SPF Can also implemented in the email gate level

PHISHING BLOCKER

The add-on includes a patent pending module for associating user credential information with specific domains. Providing a user credential to an alternate domain (e.g. other than the one the user intended) triggers a warning and submission of credentials will be blocked.

Note:
This feature contains patent pending technology

Platform Security
Front-end back-end architecture



SSL communication

Contact

Engin Yilmaz engin.yilmaz@pb.com