CitiSFT
Podręcznik Użytkownika

CitiService
Pomoc Techniczna CitiDirect
tel. 801 343 978, +48 22 690 15 21
poniedziałek – piątek; 8:00 – 17:00
helpdesk.ebs@citi.com

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

citi handlowy®

Spis treści

1.0 Cel

Niniejszy dokument przedstawia najlepsze praktyki związane z obsługą CitiSFT.

2.0 Zakres

Instrukcja dot. usług klientów zewnętrznych dostarczanych dla CitiSFT.

3.0 Przegląd i funkcje CitiSFT

Platforma (CitiSFT) to infastruktura działająca 24 godz. na dobę, zapewniająca bezpieczną metodę przesyłania plików drogą internetową między wewnętrznymi systemami Citi, a zewnętrznym klientem / systemami partnerów, wykorzystująca bezpieczne protokoły, takie jak HTTPS, FTPS i SFTP.

Utworzenie „kanałów transmisji" plików w CitiSFT między Citi a klientami wymaga utworzenia identyfikatora zarówno dla Citi, jak i dla klienta, który to proces jest zarządzany przez Citi w momencie dołączania klientów. Identyfikatory CitiSFT wspierają domyślnie uwierzytelnianie hasłem; Można również wystąpić o uwierzytelnianie oparte na kluczach SSH. Podczas pierwszego logowania identyfikatorem do interfejsu HTTPS, opartego o sieć Web wymagana jest zmiana hasła.

CitiSFT posiada także następujące możliwości:

- File Push: funkcja umożliwiająca Citi przesyłanie plików do podmiotów zewnętrznych za pomocą protokołów SFTP i FTPS
- Szyfrowanie plików z użyciem narzędzia PGP: Wsparcie dla szyfrowania PGP na poziomie pliku

4.0 Kompatybilne oprogramowanie

CitiSFT wspiera każde oprogramowanie klienta i serwera, które odpowiada poniższym standardom w celu prawidłowego działania: FTP/S (RFCs 959, 2228, i 4217), HTTP/S (RFCs 2616 i 2818), oraz SSH (RFCs 4251-4254).

4.1 Lista kompatybilnych klientów zewnętrznych

Klientci FTP

- Axway Secure Client 5.5, 5.6
- Axway SecureTransport Command Line Client (FDX) 4.5.2, 4.5.3
- Axway SecureTransport Windows Client 4.5.2
- cURL 7.19 (tylko dla HTTPS)
- CuteFTP Professional 8.3.2
- IglooFTP PRO 3.9
- Ipswitch WS_FTP 12.2
- LFTP 3.7
- SmartFTP Client 3.0

Klienci HTTP

- Apple Safari 4
- Axway Secure Client 5.5, 5.6, 5.7
- Axway SecureTransport Command Line Client (FDX) 4.5.2, 4.5.3
- Axway SecureTransport Rich Internet Client 4.9.x, 5.0, 5.1
- Axway SecureTransport Windows Client 4.5.2
- cURL 7.19
- Microsoft Internet Explorer 6 SP3, 7, 8, 9
- Mozilla Firefox 3.x, 4.x

Klienci SSH

- Axway Secure Client 5.5, 5.6, 5.7
- cURL 7.19
- FileZilla 3.3.x
- PSCP 0.60
- PSFTP 0.60
- Tectia Client 6.1
- VanDyke SecureFX 6.6.1
- WinSCP 4.2.9
- Oraz każdy klient zgodny z RFC 4251 -4254

5.0 Wspierane protokoły przesyłania

Użytkownicy uzyskują dostęp do CitiSFT za pośrednictwem poniższych bezpiecznych protokołów:

- SFTP/SCP
- FTPS
- HTTPS

Dzięki tym bezpiecznym protokołom, poświadczenia (hasła) i dane użytkownika są automatycznie szyfrowane w czasie przesyłu. W celu przesłania plików za pośrednictwem połączeń opartych o bezpieczne protokoły, użytkownicy powinni mieć możliwość połączenia się z CitiSFT za pomocą FTPS, SFTP lub HTTPS.

W przypadku ręcznego przesyłania plików, zachęcamy użytkowników do korzystania z interfejsu sieciowego CitiSFT za pośrednictwem standardowej przeglądarki wspierającej HTTPS.

CitiSFT wykorzystuje protokoły przesyłania SFTP i FTPS, nie jest to serwer FTP i nie działa w podobny sposób. Plik przesłany do CitiSFT jest natychmiast przekazywany do innej lokalizacji w celu jego przetwarzania. Po przesłaniu pliku nie należy podejmować żadnych operacji (zestawienia, zmiana, uprawnienia) na pliku lub katalogu - zakończą się one niepowodzeniem z uwagi na fakt, że plik jest przenoszony.

5.1 Przesyłanie w trybie FIPS

CitiSFT posiada tryb FIPS (Federalny standard przetwarzania informacji) dla wszystkich protokołów (HTTPS, FTPS i SFTP). Tryb FIPS wymusza użycie protokołu TLS (Transport Layer Security), a w przypadku HTTPS i FTPS wymaga aby oprogramowanie wykorzystywane przez klienta posiadało włączoną obsługę TLS v1.0.

5.2 Ogólne wytyczne konfiguracji TLS dla przeglądarek internetowych

Poniższe linki prezentują jak włączyć obsługę TLS v1.0 w popularnych przeglądarkach internetowych.

Internet Explorer: http://support.microsoft.com/kb/811834

FireFox: http://support.mozilla.org/en-US/kb/Configuring%20Firefox%20for%20FIPS%20140-2

Uwaga: Ustawienia algorytmu szyfrującego dla Internet Explorer, Google Chrome i Apple Safari są zarządzane przez system Windows i zmiana ustawień dla jednej z tych 3 przeglądarek wpłynie na inne zainstalowane na tym samym systemie. Można także zmienić te ustawienia w Panelu sterowania Windows, korzystając z ustawień Opcji Internetowych.

Internet Explorer: http://support.microsoft.com/kb/811834

Aby włączyć obsługę TLS 1.0 dla Internet Explorer należy:

1. Otworzyć menu Narzędzia, kliknąć Opcje Internetowe:
2. Wejść w zakładkę „Zaawansowane"
3. Zjechać na dół strony i zaznaczyć TLS 1.0
4. Zamknąć i uruchomić ponownie wszystkie otwarte przeglądarki.

Google Chrome:

Aby włączyć obsługę TLS 1.0 dla Chrome należy:

1. Kliknąć na ikonę klucza:
2. Wybrać Opcje
3. Wejść w zakładkę „Pod maską"
4. Kliknąć Zmień ustawienia proxy
5. Wejść w zakładkę „Zaawansowane"
6. Zjechać na dół strony i zaznaczyć TLS 1.0
7. Zamknąć i uruchomić ponownie wszystkie otwarte przeglądarki.

Apple Safari:

Aby włączyć obsługę TLS 1.0 dla Safari należy:

1. Kliknąć na ikonę ustawień (koło zębate):
2. Wybrać Preferencje
3. Wejść w zakładkę „Zaawansowane"
4. Kliknąć Ustawienia Proxy: Zmienić Ustawienia...
5. Wejść w zakładkę „Zaawansowane"
6. Zjechać na dół strony i zaznaczyć TLS 1.0
7. Zamknąć i uruchomić ponownie wszystkie otwarte przeglądarki.

Ogólne wytyczne konfiguracji CURL dla TLS

Korzystanie z TLS z wykorzystaniem biblioteki CURL: http://curl.haxx.se/libcurl/c/smtp-tls.html

Uwaga: Instrukcje dotyczące włączenia obsługi TLS dla produktu nie wymienionego w niniejszym dokumencie można uzyskać kontaktując się z dostawcą oprogramowania.

6.0 Dostęp do CitiSFT

Dostęp do CitiSFT można uzyskać za pośrednictwem poniższej w pełni kwalifikowanej nazwy domeny (FQDN), wspierającej protokoły (SFTP, FTPS, SCP i HTTPS).

Z sieci zewnętrznej do Citi:

securefiletransfer.citigroup.com

Uwaga: Klient nie powinien wykorzystywać adresów IP do łączenia się z CitiSFT. 3 systemy DNS zapewniają równoważenie obciążeń w ramach centr danych, korzystanie z FQDN jest jedynym skutecznym sposobem połączenia z CitiSFT.

6.1 Połączenie z Citi z sieci zewnętrznej

Jeżeli użytkownik zewnętrzny działa zza firewalla, należy do zapory dodać regułę umożliwiającą wysyłanie danych do środowiska CitiSFT. Grupa obsługi firewalli klientów zewnętrznych musi zezwalać na wysyłanie danych do następujących wirtualnych adresów IP (VIP) i portów.

Zewnętrzne VIP - Produkcja

192.193.218.30

199.67.137.221

Port SFTP/SCP (FTP/SCP przez SSH) 22

Port FTPS (FTP przez SSL): 21, 20444 do 21443

Port HTTPS (HTTP przez SSL): 443

Należy upewnić się, że pobieranie plików odbywa się w trybie PASYWNYM.

6.2 Klucze SSH identyfikatora hosta - Łączenie za pomocą SFTP/SCP

W przypadku hostów łączących się między sobą przez SSH, powszechne jest stosowanie procedury wymiany kluczy SSH w celu pozyskania zaufania. Wymiana taka może być automatyczna lub wywoływana za pomocą komendy, w zależności od ustawień klienta i stosowanego oprogramowania. Podczas pierwszego połączenia należy skontaktować się ze swoim administratorem systemu, który zaakceptuje wymianę. Użytkownicy SFTP muszą zaakceptować klucz SSH identyfikatora hosta w momencie pierwszego łączenia z serwerem.

Produkcja

Odcisk palca (fingerprint): 93:e6:ac:a8:e1:86:72:02:b6:68:6b:8b:65:93:f2:7f

6.3 Certyfikaty SSL - Łączenie za pomocą FTPS lub HTTPS

Platforma CitiSFT jest skonfigurowana tak aby korzystać z certyfikatów SSL podpisanych przez Verisign dla protokołów FTPS i HTTPS. Takie certyfikaty wygasają okresowo. Jeżeli użytkownicy chcą zautomatyzować przesyłanie plików przez FTPS i/lub HTTPS, zaleca się korzystanie z zaufanego centrum certyfikacji Verisign oraz certyfikatów pośredniczących, jako że te posiadają przedłużoną datę wygaśnięcia.

Najczęściej stosowane przeglądarki internetowe automatycznie aktualizują swoje listy certyfikatów z serwerem głównym i pobierają aktualne certyfikaty pośredniczące, wystawiane przez wystawców (CA), jak np. Verisign. Użytkownikom chcącym zautomatyzować obsługę FTPS i/lub HTTPS, zaleca się korzystanie z centrum certyfikacji Verisign oraz certyfikatów pośredniczących. Aby dowiedzieć się w jaki sposób importować/dodać do zaufanych certyfikat Verisign i certyfikaty pośredniczące, należy skontaktować się ze swoim administratorem systemu lub zespołem pomocy technicznej klienta oprogramowania.

Zaufane certyfikaty pośredniczące weryfikacji rozszerzonej Verisign Pro SSL (Wydzielone certyfikaty CA / Premium SSL z EV / RSA SHA-1):

http://www.verisign.com/support/verisign-intermediate-ca/extended-validation-pro/index.html

Zaufany certyfikat główny G5 klasy 3 Verisign:

http://www.verisign.com/support/roots.html

6.4 Pierwsze zmiany hasła

W celu aktywacji konta w CitiSFT, pierwsze logowanie musi odbyć się za pośrednictwem interfejsu sieciowego HTTPS. W trakcie tego logowania zostaną Państwo poproszeni o zmianę hasła tymczasowego, dostarczonego przez HelpDesk.

Z sieci zewnętrznej do Citi:

https://securefiletransfer.citigroup.com

Jeżeli chcą Państwo zmienić hasło po pierwszym logowaniu, należy wykonać poniższe czynności:

1. Zalogować się do CitiSFT za pomocą protokołu HTTPS.
2. Na ekranie transferu kliknąć My account
3. Wpisać stare hasło.
4. Wpisać nowe hasło i potwierdzić je.
5. Kliknąć Set Password.

6.5 Uwierzytelnianie oparte na kluczach SSH

Uwierzytelnianie oparte na kluczach SSH jest opcjonalne i wspierane jedynie w przypadku korzystania z SFTP. Klucze muszą być w formacie RSA. Klucze DSA nie są wspierane. W przypadku włączonego uwierzytelniania opartego na kluczach, klient powinien widzieć katalog sshkey na swoim koncie. Po włączeniu obsługi uwierzytelniania opartego na kluczach dla konta, w katalogu użytkownika pojawi się katalog „sshkeys".

- Użytkownik musi zmienić PUBLICZNĄ część klucza na „klucze_autoryzowane" *[authorized_keys]* a następnie przesłać go do katalogu „sshkeys" z wykorzystaniem interfejsu HTTPS. Należy się upewnić, że wykorzystywany jest tryb ASCII. Klucze PRYWATNE powinny być przechowywane przez użytkownika i nigdy nie przesyłane do CitiSFT.
- Aby zweryfikować konfigurację należy zalogować się do CitiSFT za pomocą SFTP i przeprowadzić uwierzytelnianie oparte na kluczach. Logowanie powinno być możliwe bez konieczności wprowadzania haseł.

Jeżeli uwierzytelnianie oparte na kluczach zakończy się niepowodzeniem, użytkownik zostanie poproszony o podanie hasła. Jeżeli proces łączenia z CitiSFT jest zautomatyzowany, należy się upewnić, że wprowadzono poprawne hasło na wypadek niepowodzenia uwierzytelniania opartego na kluczach.

6.6 Ograniczenie źródłowych adresów IP

CitiSFT oferuje dodatkową funkcję, umożliwiającą ograniczenie dostępu jedynie dla zdefiniowanych adresów (adresu) IP klientów. Szyfrowanie/Odszyfrowywanie PGP na poziomie pliku.

7.0 Szyfrowanie/Odszyfrowywanie PGP na poziomie pliku

Szyfrowanie PGP na poziomie pliku to opcjonalna funkcja dostępna w CitiSFT w celu zapewnienia (tam gdzie to konieczne) dodatkowego zabezpieczenia operacji przesyłania pliku. Rozmiar plików, wymagających szyfrowania/odszyfrowywania PGP nie może przekraczać 500MB. Jeżeli istnieje konieczność przesłania większego pliku z wykorzystaniem szyfrowania PGP, zaleca się podział pliku na części o rozmiarze nieprzekraczającym 500MB i przesłanie ich jako osobnych plików.

Uwaga: Aby uzyskać publiczny klucz PGP Citi, należy skontaktować się z HelpDeskiem Bankowości Elektronicznej.

7.1 Wybór produktu PGP

Klient powinien używać produktów PGP ograniczających algorytmy szyfrujące jedynie do algorytmów zgodnych ze standardem FIPS 140-2.

CitiSFT zaleca dowolne oprogramowanie PGP zgodne z RFC 4880, Użytkownicy muszą posiadać wspierane na bieżąco oprogramowanie PGP, obsługujące algorytmy AES256 i SHA256. Przykładem mogą być GPG 1.4+, PGP 10+, lub jakikolwiek produkt równoważny, który spełnia te zalecenia.

8.0 Nazewnictwo plików

Nazewnictwo plików należy omówić z właścicielem procesu w Citi Handlowy w celu upewnienia się, że zastosowano odpowiedni prefiks pliku. Prefiks pliku to znaki na początku nazwy pliku, z rozróżnieniem wielkości liter (zalecana długość: do 15 znaków).

W przypadku zastosowania nierozpoznanego prefiksu, CitiSFT usunie plik. Następnie zostanie wysłane powiadomienie e-mail do odbiorców skonfigurowanych podczas instalacji. Dalsze szczegóły patrz: punkt 13.0 Powiadomienia e-mail poniżej.

8.1 Znaki obsługiwane w nazwach plików

Dopuszczalna długość nazwy pliku w CitiSFT wynosi 100 znaków i musi składać się z poniższych znaków:

A-Z

a-z

0-9

._-()#

Użycie **Spacji** i poniższych znaków w nazwie pliku skutkować błędami i nie gwarantujemy powodzenia operacji przesyłania w przypadku zastosowania poniższych znaków:

& ; : ` , \ | " * ? ~ < > ^ [ ] { } $ @ %

9.0 Dzienny limit wysyłania

Domyślnie platforma CitiSFT umożliwia przesłanie do **1 GB** łącznych danych, wysłanych przez jednego nadawcę dziennie (od godz. 00:00 do 23:59 czasu wschodniego). Jeżeli klient wymaga zwiększonego przydziału dziennego, powienien skontaktować się z HelpDeskiem Bankowości Elektronicznej. Polityka przechowywania plików

Podczas tworzenia kont w CitiSFT domyślny okres przechowywania pliku adresata (adresatów) wynosi 24 godziny. Możliwa jest zmiana okresu przechowywania plików adresata na 2, 5 lub 7 dni.

W momencie przesłania do CitiSFT, plik o danej nazwie każdorazowo nadpisuje istniejący plik o tej samej nazwie. W przypadku klientów korzystających z automatycznego nazewnictwa plików, zaleca się stosowanie unikalnych nazw plików, np. poprzez umieszczanie w nich sygnatury czasowej.

Alternatywnym sposobem na wydłużenie okresu przechowywania plików jest skorzystanie z dostępnej w CitiSFT funkcji File Push, która automatycznie wypchnie pliki na serwer klienta za pośrednictwem protokołów SFTP lub FTPS.

10.0 File Push (usługa wysyłania pliku)

CitiSFT zawiera opcję Push, dzięki której pliki mogą być wypychane do serwera docelowego, pod warunkiem, że dany serwer akceptuje połączenia FTPS i/lub SFTP. Funkcja Push CitiSFT bierze kopię pliku wysłanego na konto adresata i dostarcza plik na serwer docelowy, wskazany podczas uruchamiania procesu.

10.1 Wymagania usługi Push

Serwery Push muszą obsługiwać komunikację opartą na FTPS i/lub SFTP. Jeżeli istnieje konieczność przesłania pliku w formacie ASCII (zamiast w domyślnym formacie binarnym), opcję tą należy zaznaczyć w Państwa żądaniu dotyczącym CitiSFT.

Identyfikator / Hasło użytkownika Push

Identyfikator / Hasło użytkownika na serwerze Push „nie może" zawierać żadnych znaków powłoki, takich jak m.in.: „@", „$", „>", "`", "(", ")", i „<".

Katalog Push

Identyfikator Push powinien posiadać uprawnienia do odczytu i zapisu w swoim katalogu Push.

Uwierzytelnianie oparte na kluczach SFTP (Klucze Push)

Jeżeli chcą Państwo korzystać z uwierzytelniania opartego na kluczach SFTP, prosimy ***o kontakt z HelpDeskiem Bankowości Elektronicznej*** w celu uzyskania odpowiedniego klucza publicznego.

10.2 Reguły firewalla dla usługi File Push

CitiSFT korzysta z serwerów proxy w celu wysyłania plików do klientów zewnętrznych przez Internet. Klienci Zewnętrzni powinni umożliwiać połączenia wychodzące z niniejszych (poniższych) serwerów proxy oraz zapewniać odpowiednie trasowanie (routing) dla ruchu zwrotnego.

Źródłowy adres IP:

192.193.216.0/24 (192.193.216.1 to 192.193.216.255) - południowo zachodnia pula proxy

199.67.131.128/27 (199.67.131.129 to 199.67.131.158) - środkowo zachodnia pula proxy

199.67.131.192/27 (199.67.131.193 to 199.67.131.222) - środkowo zachodnia pula proxy

Docelowy adres IP:

Adres(y) IP serwera klienta

Port:

Port(y) TCP wymagany(e) do nasłuchiwania usługi SFTP lub FTPS po stronie serwera klienta.

Uwaga: Docelowy adres IP i Port są zależne od konfiguracji serwera klienta. Portem domyślnym dla SFTP jest TCP/22, dla FTPS jest TCP/21. Należy też zauważyć, że w przypadku FTPS wykorzystywany jest tryb pasywny.

11.0 Powiadomienia e-mail

CitiSFT może wysyłać wiadomości e-mail dotyczące Powodzenia lub Niepowodzenia na wiele adresów e-mail i/lub list dystrybucyjnych, w tym na zewnętrzne adresy e-mail. Powiadomienia e-mail muszą zawierać prawidłowy adres e-mail. Lista dystrybucyjna MS Exchange ani nazwy folderu publicznego nie są wspierane.

CitiSFT generuje 5 rodzajów powiadomień e-mail dla użytkowników; nadawcą jest „Transfer":

1. E-mail o Niepowodzeniu przesyłania (temat zaczyna się frazą „Transfer FAULT!")
2. E-mail o Powodzeniu przesyłania (temat zaczyna się frazą „Transfer PASS")
3. E-mail o Niepowodzeniu pobierania
4. E-mail o Powodzeniu pobierania
5. Nieprawidłowy prefiks pliku (wysyłany jedynie do właścicieli kont)

CitiSFT wysyła powiadomienie e-mail w przypadku zaistnienia jednego z poniższych scenariuszy.

1. Plik przekracza dozwolony rozmiar: CitiSFT wysyła „E-mail o Niepowodzeniu", informujący, że przekroczony został dopuszczalny rozmiar pliku.
2. Błąd przetwarzania: CitiSFT wysyła „E-mail o Niepowodzeniu", informujący o przyczynie niepowodzenia transferu - system nieosiągalny, błąd funkcji konta, nie odnaleziono ścieżki docelowej, (system not reachable, functional account failed, destination path not found, etc.).
3. Przetwarzanie zakończone Powodzeniem: CitiSFT wysyła „E-mail o Powodzeniu".
4. Plik pobrany: CitiSFT wysyła powiadomienia o pobraniu.
5. E-mail dotyczący plików o rozmiarze zero bajtów: CitiSFT może informować użytkowników o przesłaniu przez nich pliku o rozmiarze zero bajtów.
6. Nieprawidłowy prefiks pliku: CitiSFT wysyła powiadomienie e-mail do właściciela konta. Należy zauważyć, że e-mail informuje o nieodnalezionej trasie, tj. użyty prefiks nie połączył się z prawidłową trasą(Note that the email indicates route not found- i.e. prefix used does not link to a valid route).

Uwaga: Jeśli chcą Państwo otrzymywać takie powiadomienia, należy taka potrzebę uwzględnić na etapie wypełniania wniosku aktywacyjnego.

12.0 Przesyłanie plików w Citi SFT - Instrukcja krok po kroku

12.1 Wychodzący transfer plików (z Citi do Klienta)

1. Nadawca (pracownik Citi) nadaje plikowi odpowiednią nazwę, np. Prefixfilenamedata(ddmmrrrr).xls.
2. Nadawca (pracownik Citi) loguje się do CitiSFT, ręcznie lub za pośrednictwem zewnętrznego programu / skryptu do przesyłania plików, ze swojego konta CitiSFT i przesyła plik.
3. Jeżeli transfer wykorzystuje szyfrowanie PGP, CitiSFT automatycznie szyfruje plik za pomocą publicznego klucza PGP klienta i podpisuje go prywatnym kluczem PGP Citi.
4. CitiSFT przesyła pliki do katalogu macierzystego odbiorcy (Klienta) w CitiSFT.
5. Odbiorca (klient) loguje się do CitiSFT, ręcznie lub za pośrednictwem zewnętrznego programu / skryptu do przesyłania plików, ze swojego konta i pobiera plik.
6. Jeżeli transfer wykorzystuje szyfrowanie PGP, odbiorca (klient) zweryfikuje podpis CitiSFT wykorzystując publiczny klucz PGP CitiSFT, a po zakończeniu tego procesu odszyfruje plik za pomocą swojego klucza prywatnego.
7. Jeżeli transfer wykorzystuje funkcję Push, CitiSFT wyśle plik to serwera docelowego klienta. Dzięki tej funkcji klient może pominąć krok 5. Jeśli jednak serwer klienta jest niedostępny, wówczas klient ma nadal możliwość ręcznego pobrania pliku, postępując zgodnie z krokiem 5.

12.2 Przychodzący transfer plików (od Klienta do Citi)

1. Nadawca (klient) nadaje plikowi odpowiednią nazwę, np. Prefixfilenamedata(ddmmrrrr).xls.
2. Jeżeli transfer wykorzystuje szyfrowanie PGP, nadawca (klient) zaszyfruje plik za pomocą publicznego klucza PGP CitiSFT i podpisze go swoim prywatnym kluczem PGP. Proces ten należy wykonać w obrębie jednego procesu PGP.
3. Nadawca (klient) loguje się do CitiSFT, ręcznie lub za pośrednictwem zewnętrznego programu / skryptu do przesyłania plików, ze swojego konta i przesyła plik.
4. Jeżeli transfer wykorzystuje odszyfrowywane PGP, CitiSFT automatycznie weryfikuje podpis wykorzystując publiczny klucz PGP klienta, a po zakończeniu tego procesu odszyfruje plik za pomocą prywatnego klucza CitiSFT.
5. CitiSFT przesyła pliki na konto katalogu odbiorcy (pracownika Citi).
6. Odbiorca (pracownik Citi) loguje się do CitiSFT, ręcznie lub za pośrednictwem zewnętrznego programu / skryptu do przesyłania plików, ze swojego konta i pobiera plik.

13.0 Kontakt w sprawie pomocy technicznej

1. HelpDesk Bankowości Elektronicznej.

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

citi handlowy®