
asseco
DATA SYSTEMS

asseco DATA SYSTEMS

Certyfikaty Certum eMail ID S/MIME

w kontekście bezpiecznej pracy zdalnej

Kwiecień, 2020

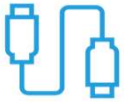
Certum eMail ID (S/MIME)

asseco DATA SYSTEMS

S / MIME (Secure /Multipurpose Internet Mail Extensions) to powszechnie akceptowany protokół wysyłania **podpisanych cyfrowo i zaszyfrowanych wiadomości**

Szyfrowanie wiadomości

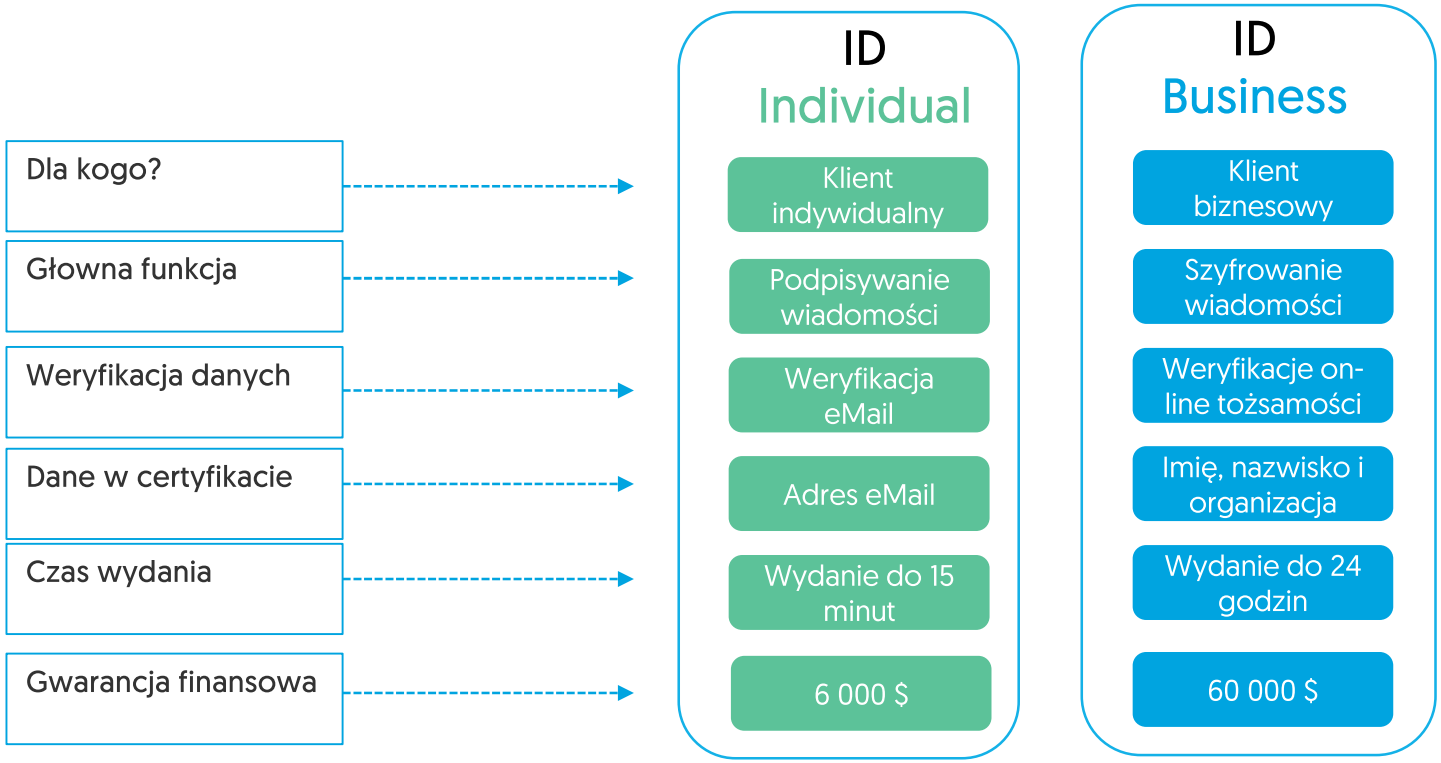
Podpisywanie wiadomości



Uwierzytelnienie użytkowników

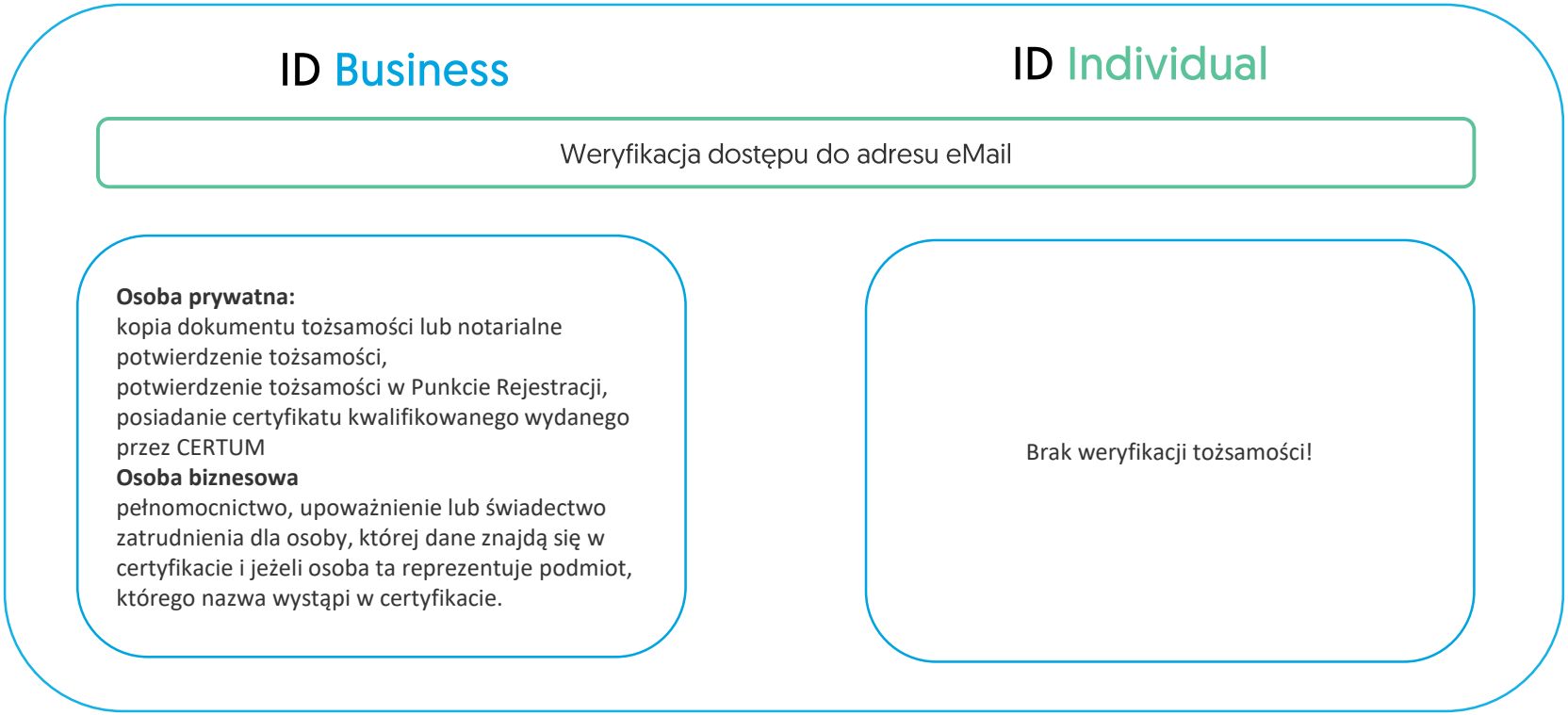
Warianty wydania

Oba certyfikaty można kupić na okres 1,2 i 3 lat. Różnicę między wariantami stanowi sposób weryfikacji oraz dane w certyfikacie



Weryfikacja certyfikatów

Weryfikacja jest w pełni zdalna i nie wymaga kontaktu F2F

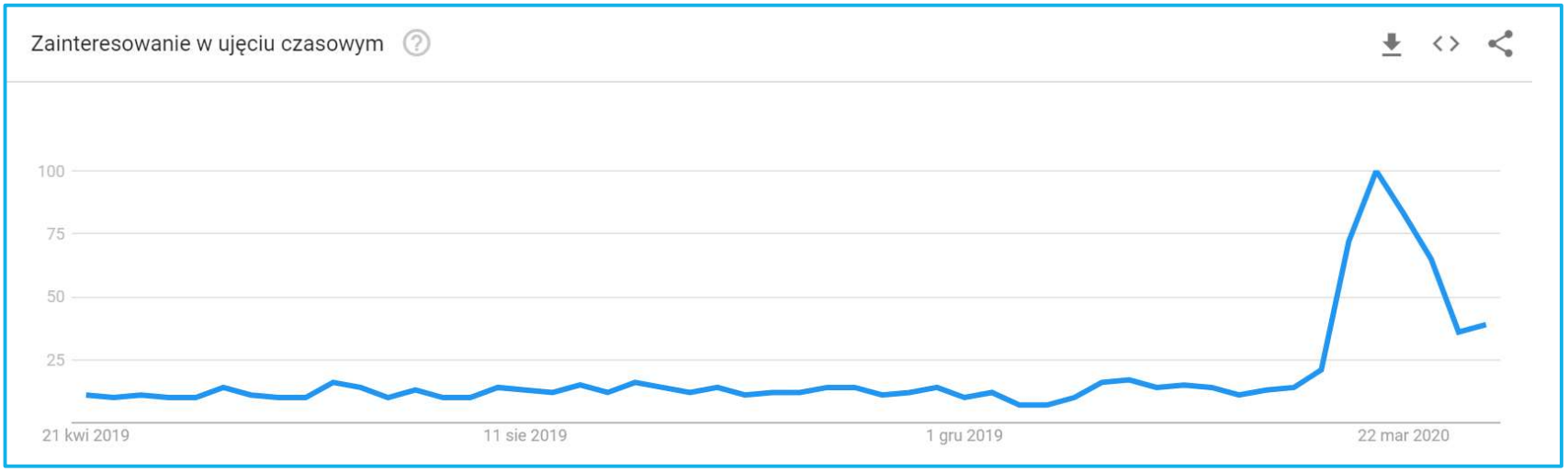


Szyfrowanie maili z Certum ID (S/MIME)

Poufność korespondencji - szyfrowanie wiadomości oparte na modelu end-to - end

Szyfrowanie maili w kontekście pracy zdalnej

Zgodnie z Google Trends zainteresowania szyfrowaniem maili znacznie wzrosło w ostatnim czasie.



Szyfrowanie maili w kontekście pracy zdalnej

Firmy i instytucje interesują się certyfikatami S/MIME w kontekście pracy zdalnej

Bezpieczna komunikacja

- # Nie przesyłaj służbowych informacji za pomocą publicznych komunikatorów internetowych takich jak Messenger, Face Time, Hangouts, itp..
- # Zachowaj ostrożność przy odbieraniu wiadomości pocztowych – zwracaj uwagę na adres nadawcy wiadomości, czy treść wiadomości nie budzi podejrzenia, nie klikaj w podejrzane linki i nie otwieraj podejrzanych załączników.
- # Nie wysyłaj materiałów służbowych na prywatne konta e-mailowe.
- # Zwracaj szczególną uwagę na wiadomości pocztowe, których nadawcą jest osoba spoza organizacji o nazwie zgodnej z nazwiskiem użytkownika Asseco Data Systems. Na przykład pod użytkownika adam.kowalski@assecods.pl może podszywać się adam.kowalski@asceccods.pl.
- # Szyfruj i podpisuj e-maile imiennym certyfikatem poczty tam gdzie to możliwe. Instrukcję instalacji certyfikatu znajdziesz na Intranecie:

Dlaczego szyfrowanie jest dobrym pomysłem na zabezpieczenie poczty podczas pracy zdalnej?

- ✓ Szyfrowanie z S/MIME działa poza siecią w przeciwieństwie do wielu innych dostępnych narzędzi DLP opartych na infrastrukturze serwer-klient
- ✓ Podstawowy certyfikat Certum ID Individual jest dostępny do użycia do 15 minut po zakupie
- ✓ Certyfikaty ID nie wymagają wdrożenia. Programy DLP, które chronią pocztę wymagają nawet do kilku tygodni konfiguracji
- ✓ Certyfikaty S/MIME są proste w implementacji, każdy użytkownik może wdrożyć certyfikat w kilka minut
- ✓ Certyfikaty uczą dobrych praktyk pracy z pocztą elektroniczną

Zabezpieczenie komunikacji w organizacji

Firma X z sektora medycznego zgłosiła się, aby zabezpieczyć maile zawierające dane osobowe z użyciem skrzynki pocztowej Thunderbird, zaznaczając, że główne problemy z którymi się mierzą to:

- × Zaadresowania poczty do niepoprawnego adresata – dane osobowe trafią do pracownika, który nie ma do nich dostępu
- × Przechwycenie wiadomości przez osoby trzecie
- × Zapisanie/praca na danych poza komputerem służbowym z użyciem skrzynki webowej – dane zostaną zapisane na komputerze osobistym, który nie jest tak zabezpieczony, jak komputer służbowy

Jak S/MIME zabezpieczył i rozwiązał problem z wymianą korespondencji poufnej?

- ✓ Zaszyfrowane dane mogą wymieniać tylko nadawca i odbiorca, którzy posiadają klucz publiczny potrzebny do odszyfrowania wiadomości. W momencie, kiedy wiadomość trafi do osoby, z którą nie został wymieniony klucz publiczny nie odczyta ona maila.
- ✓ Zaszyfrowaną wiadomość można odczytać tylko i wyłącznie na komputerze, gdzie jest wgrany certyfikat. Pracownik nie będzie miał dostępu do zaszyfrowanej poczty poza miejscem pracy.
- ✓ Certyfikaty są obsługiwane tylko przez autoryzowane i zaufane skrzynki pocztowe dzięki czemu pracownik logujący się na skrzynkę webową nie pobierze danych w sposób nieautoryzowany.

Zabezpieczenie komunikacji handlowej

Firma handlowa zwróciła się do nas z problem braku zabezpieczeń na linii wymiany maili między handlowcem a klientem.

Jakie ryzyka czyhają na klienta i handlowca w obliczu braku zabezpieczeń?

- × narażenie na utratę danych osobowych
- × narażenie danych poufnych na wyciek
- × narażenie danych na przechwycenie przez konkurencję
- × utrata wizerunku

Jak S/MIME rozwiązuję problem?

Firma handlowa kupuje kilkanaście sztuk certyfikatów ID, a następnie z poziomu swojego konta Certum przekazuje certyfikaty swoim klientom. Koszt certyfikatu wlicza w koszt projektu. Dzięki certyfikatom korespondencja zachowa poufność i będzie dostępna tylko i wyłącznie na komputerach z certyfikatem. Jeśli handlowiec lub klient korzysta z więcej niż jednego urządzenia warto rozważyć zakup certyfikatu z kartą. Wtedy odczyta swoje wiadomości wszędzie, gdzie będzie ale tylko i wyłącznie w czasie użycia karty.

Zabezpieczenie komunikacji w dobie pracy zdalnej jest jednym z najważniejszy elementów stworzenia bezpiecznej przestrzeni dla pracowników. Pracując poza miejscem pracy, często zmieniając środowisko, sieć i komputery muszą posiadać łatwe we wdrożeniu narzędzie, które zabezpieczy komunikację.

Oprócz zabezpieczenia komunikacji wewnętrznej należy pamiętać o zabezpieczaniu komunikacji wymienianej spoza osobami z firmy. Jest to szczególnie ważne w dobie pracy zdalnej, kiedy pracownicy pracują poza siecią i nie wiemy, czy dysponują bezpiecznym połączeniem WI-FI.

Dlaczego warto szyfrować pocztę z S/MIME?

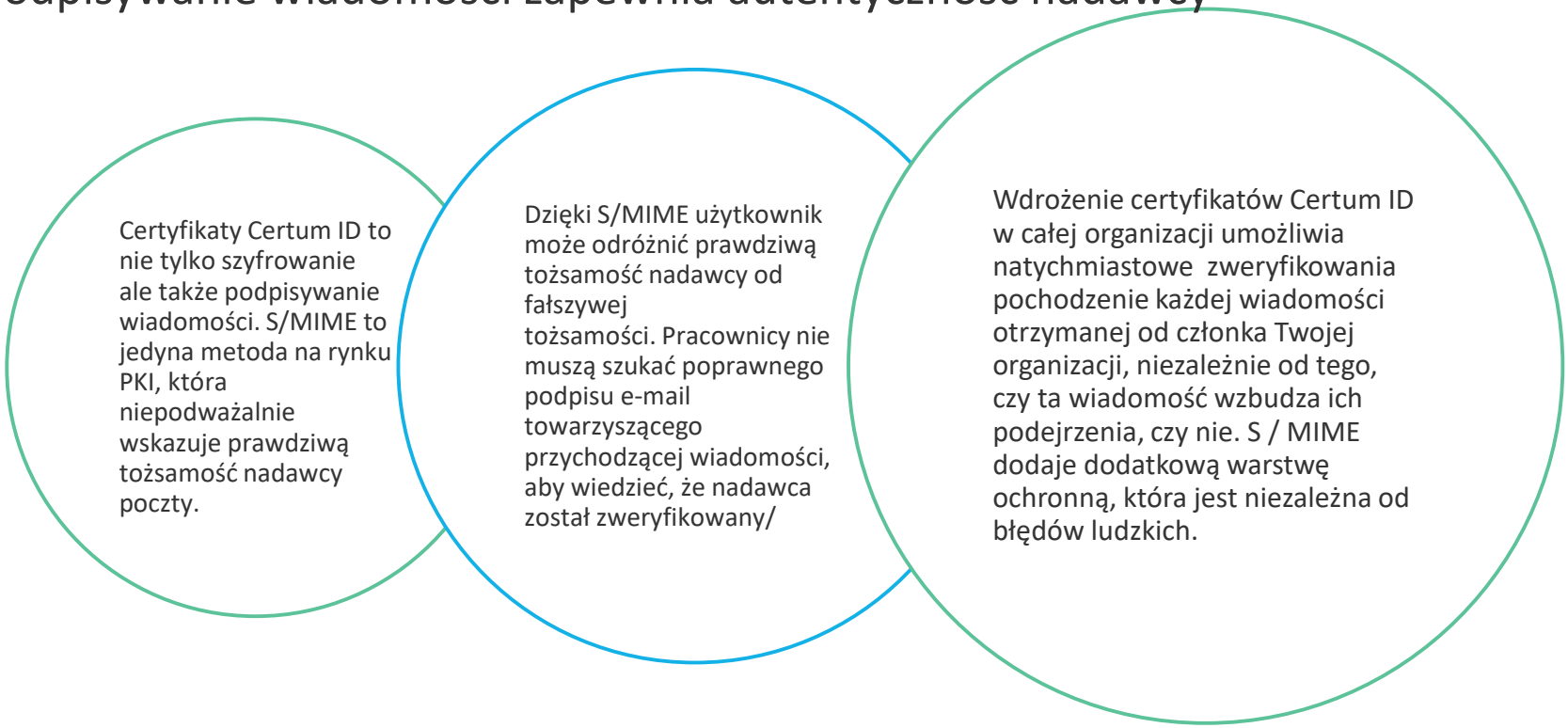
Funkcja szyfrowania użyta wewnątrz organizacji pozwala na budowanie wiarygodnej polityki bezpieczeństwa

Zachowanie poufności i prywatności

- Zaszyfrowane maile zostaną odczytane tylko przez osobę, która posiada klucz pracujący do klucza nadawcy
- Wysyłane załączniki zostaną odpowiednio zabezpieczone przed wyciekiem
- Przesyłana treść nie zostanie zmodyfikowana przez niepowołane osoby
- Zapewnia zgodność z RODO w organizacjach
- Zapobiega fałszowaniu eMail

Podpisywanie wiadomości

Podpisywanie wiadomości zapewnia autentyczność nadawcy



Podpisywanie wiadomości w czasach COVID-19

W zeszłym tygodniu Google odnotowało ponad 18 milionów wiadomości e-mail ze złośliwym oprogramowaniem i phishingiem związanych z COVID-19. Najczęściej atakowane są organizacje. Cyfrowi przestępcy podszywają się pod zespoły helpdeskowe, HR i marketingowe.

- ✓ Dzięki S/MIME wiadomości podpisane zyskują wizualną reprezentacji w postaci ikony kotyliona przy nadawcy. Dzięki temu wiesz, że wiadomość została zweryfikowana i pochodzi od tego, kto ją wysyła.
- ✓ Ponadto certyfikaty biznesowe udzielają również informacji firmowych zapewniając oficjalne uwierzytelnienie nadawcy.
- ✓ Jeśli nadawca wiadomości e-mail odpowiednio podpisze swoją wiadomość, partner komunikacji będzie mógł sprawdzić, czy jest to „prawdziwy” fałszywy e-mail. Jeśli wiadomość e-mail nie została podpisana, należy zachować ostrożność z zawartością.

Zabezpieczenie przed phishingiem

W Firmie Y kilkanaście komputerów zostało zainfekowanych wirusem ransomware. Wirus przedostał się do biura za pomocą załącznika e-mail.

Skutki zainfekowania komputerów:

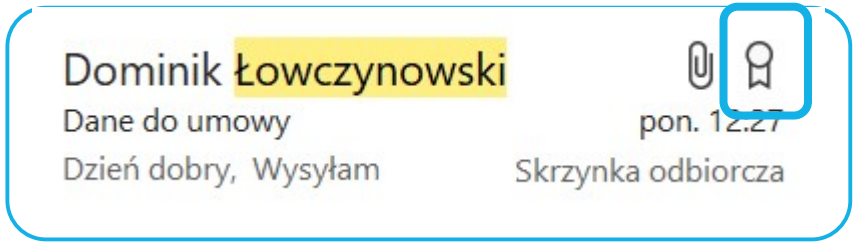
- × Utrata danych wskutek zarażenia złośliwym oprogramowaniem
- × Spowolnienie pracy komputerów
- × Przestój w pracy firmy – konsekwencje finansowe
- × Utrata zaufania - Narażenie klientów na zainfekowania ransomwere

Jak można było się ustrzec przed taką sytuacją?

Dobry program antywirusowy to nie wszystko. S/MIME rozwiązuje problem phishingu w najprostszy możliwy sposób: dostarczając niepodważalne dowody na tożsamość nadawcy.

Po implementacji i wymiany klucza, pracownicy będą mogli automatycznie podpisywać pocztę z poziomu aplikacji pocztowych. Podpisana pocztą od razu się wyróżnia wśród setek maili dzięki ikonie kotyliona i uwierzytelnia nadawcę za pomocą wskazania jej danych osobowych.

Wielu przestępców wykorzystuje obecną sytuację celem zainfekowania jak największej ilości komputerów złośliwym oprogramowaniem. Wykorzystując brak czujności pracowników pracujących w domowym zaciszu podszywają się pod osoby z organizacji i wymuszają kliknięcie linka znajdującego się w mailu. Celem każdej organizacji jest umożliwienie pracownikom łatwego rozpoznania wiadomości pochodzącej od zaufanego odbiorcy. Dzięki S/MIME wiadomości zyskują wizualną reprezentację:



Dlaczego warto podpisywać pocztę z S/MIME?

Cyfrowy podpis to funkcjonalność Certyfikatu ID, która pozwala potwierdzić autentyczność wysłanych wiadomości

Budowanie tożsamości osobistej i biznesowej w sieci

- W zależności od wariantu wydania certyfikatu, wiadomości zawsze będą podpisane
- Potwierdzenie niezaprzeczalności pochodzenia – Ochrona przed phishingiem
- Budowanie zaufania za pomocą dodatkowych danych
- Uwiarygodnienie i potwierdzenie rzetelności Twojej firmy

Uwierzytelniania użytkowników

W czasach zwiększonej mobilności i pracy poza biurem warto pomyśleć, czy nie warto zabezpieczać komputerów pracowników dodatkową warstwą ochrony.

Prosta funkcyjność logowania się do systemów

- Prosta do konfiguracji kontrola dostępu do systemów
- Bezpieczny dostęp do aplikacji tylko dla autoryzowanych osób
- Jedno hasło do wielu systemów

O czym warto jeszcze wiedzieć?

Warunki korzystania z certyfikatów S/MIME

Warunkiem szyfrowania wiadomości jest posiadania przez nadawcę i odbiorcę certyfikatu.

Po skonfigurowaniu S / MIME należy jednorazowo dokonać wymiany cyfrowo podpisanych wiadomości e-mail z odbiorcą. Umożliwi to wysyłanie zaszyfrowanych wiadomości e-mail.

Certyfikaty S/MIME przeznaczone są dla programów pocztowych

Certyfikaty S/MIME nie będą działać poprawnie na pocztach uruchamianych przez przeglądarkę!

Wyjątkiem jest poczta gmail.com z wykupionym dostępem do pakietu G-Suite oraz poczta webowa Outlook, która po odpowiedniej konfiguracji umożliwi korzystanie z certyfikatu.

Siła tworzenia.

www.assecods.pl

asseco DATA SYSTEMS