

LEGAL & COMPLIANCE

W



- Najważniejsze pytania i odpowiedzi -

Platforma Autenti

to unikalne połączenie podpisu elektronicznego oraz innowacyjnej technologii w ramach europejskiego i krajowego środowiska prawnego.

Wykorzystujemy zaawansowane technologie bezpieczeństwa, aby szybko, skutecznie i wygodnie zawierać umowy i podpisywać dokumenty, a w razie sporu dysponować dowodami na złożenie podpisów.

Spis treści

Spis treści.....	2
1. Dlaczego podpisywanie przez platformę Autenti jest zgodne z prawem?	4
2. W oparciu o jakie przepisy prawa i/lub rekomendacje działa Autenti?	4
3. Jakie dokumenty regulują usługi oferowane przez Autenti?	4
4. Co znaczy sformułowanie “zaufana strona trzecia”?.....	4
5. Na jakiej podstawie Autenti staje się “zaufaną stroną trzecią”?.....	5
6. Kto lub co potwierdza, iż Autenti jest usługą zaufania? Czy Autenti posiada wszystkie wymagane prawem zezwolenia lub koncesje?	5
7. Jakie dowody otrzymują podpisujący dokumenty dzięki Autenti?	5
8. Dlaczego potwierdzenia Autenti są skutecznym dowodem?	5
9. Czym jest podpis elektroniczny?	6
10. Czym jest rozporządzenie eIDAS?.....	6
11. Kiedy podpis elektroniczny na dokumentach jest ważny?.....	6
12. W jaki sposób Autenti zabezpiecza interesy podpisujących stron?	6
13. Czym jest Karta Podpisów Autenti?	7
14. Co to znaczy, że dokumenty podpisane elektronicznie przez Autenti są prawnie wiążące?.....	7
15. Czym jest gwarancja dostępności treści?	8
16. W jaki sposób gwarantowana jest niezmienność (integralność) treści?	8
17. Na czym polega znakowanie czasem dokumentów elektronicznych i jakie zastosowanie ma kwalifikowany elektroniczny znacznik czasu?.....	8
18. Czym jest i na jakiej podstawie Autenti spełnia wymagania dotyczące trwałego nośnika?	8
19. Czym jest i w jaki sposób gwarantowana jest autentyczność pochodzenia dokumentu oraz jego integralność?	9
20. Od czego zależy i jak wybrać właściwy rodzaj podpisu elektronicznego?	9
21. Jakie są formy składania oświadczeń woli i do których mogę użyć podpisu elektronicznego?.....	9
22. Jaka jest różnica pomiędzy formą pisemną a dokumentową?.....	10
23. Które dokumenty mogę podpisywać podpisem elektronicznym (e-podpisem Autenti), a do których niezbędne będzie użycie kwalifikowanego podpisu elektronicznego (opcja także dostępna w ramach platformy Autenti)?	10
24. Czy mogę za pomocą platformy Autenti podpisywać dokumenty z osobami z zagranicy? Jak w takim przypadku będzie się miał do tego regulamin Autenti i przepisy prawa?	10
25. Jak weryfikowane są osoby podpisujące dokumenty na platformie Autenti?	10
26. W jaki sposób Autenti weryfikuje używane na platformie podpisy?	11
27. RODO a Autenti – czy następuje transfer danych osobowych poza Europejski Obszar Gospodarczy? ..	11
28. Kto może złożyć podpis elektroniczny?	11
29. Skąd wiadomo kto podpisał dokument?	11
30. Na jakiej podstawie Autenti przetwarza dane osobowe stron?	11

31. Dlaczego przechowywanie dokumentów podpisanych na platformie jest bezpieczne?	11
32. Kto korzysta z rozwiązań Autenti?	12
33. Jaką infrastrukturę wykorzystuje Autenti do świadczenia usług?	12
34. Gdzie zlokalizowane są centra danych w których są zapisywane dokument podpisane przez Autenti?.....	12
35. Czy dokumentami podpisanymi elektronicznie można posługiwać się w sprawach sądowych?	12
36. Czy dokumenty podpisane elektronicznie mogą być wykorzystywane w relacjach międzynarodowych?.....	12
37. Jak długo przechowywane są dokumenty na platformie Autenti?	13
38. Kto ma dostęp do dokumentów podpisanych na platformie Autenti?	13
39. Jak dopasować treść dokumentów podpisywanych elektronicznie do tego trybu składania oświadczeń woli (przykłady)?.....	13
40. W jaki sposób Autenti zarządza incydentami bezpieczeństwa?	13
41. Jakie procedury Autenti stosuje w zakresie zarządzania ryzykiem bezpieczeństwa informacji?	13
42. Czy Autenti posiada stosowne ubezpieczenie odpowiedzialności cywilnej (OC)?	14
43. Czy Autenti wprowadziło i utrzymuje polityki / procedury mające na celu przeciwdziałanie praniu pieniędzy, finansowaniu terroryzmu, łapownictwu i korupcji?	14
44. Jak Autenti realizuje zobowiązanie do zachowania w tajemnicy Informacji Poufnych?	14
45. Jak wyglądają procedury BCP w Autenti?.....	14
46. Jak Autenti realizuje usługi wsparcia technicznego i SLA?.....	14
47. Czy Autenti działa zgodnie z normami PN- ISO/IEC ISO 20000, PN -EN ISO/IEC 27001, PN-EN ISO 22301; ISO/IEC 27017 lub ISO/IEC 27018?	14
48. Czy Autenti gwarantuje bezpieczeństwo sieci w ramach swojej działalności?.....	14
49. Jakie testy penetracyjne wykonuje Autenti?.....	15

1. Dlaczego podpisywanie przez platformę Autenti jest zgodne z prawem?

Zgodnie z polskim i europejskim prawem, do skutecznego zawarcia umowy nie jest konieczny wymagany klasyczny podpis na papierze, chyba, że istnieje wyraźnie wskazany wyjątek przewidziany przepisami prawa. Zgodnie z art. 60 k.c., dla złożenia oświadczenia woli wystarczy jakiegokolwiek zachowanie się danej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej.

Platforma Autenti oferuje zarówno możliwość zastosowania formy dokumentowej (podpis elektroniczny / e-podpis Autenti) – czyli takiej, która jest wystarczająca wówczas, gdy prawo nie wymaga formy szczególnej oraz formy elektronicznej (kwalifikowany podpis elektroniczny), jeżeli dla ważności danej czynności konieczne jest zachowanie formy pisemnej.

Zgodnie z prawem europejskim wszystkie rodzaje podpisu elektronicznego są ważne, niezależnie od tego, czy zostały opatrzone kwalifikowanym certyfikatem. W związku z tym, podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych (art. 25 ust. 1 Rozporządzenia eIDAS). Kwalifikowane podpisy elektroniczne mają natomiast skutek podpisu własnoręcznego (art. 25 ust. 2 Rozporządzenia eIDAS).

Podpis elektroniczny złożony pod oświadczeniem woli zawsze zapewnia zachowanie formy dokumentowej, co pozwala na skuteczne zawarcie większości umów funkcjonujących w obrocie gospodarczym.

2. W oparciu o jakie przepisy prawa i/lub rekomendacje działa Autenti?

Autenti świadczy usługi zaufania w oparciu o Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE zwaną eIDAS, a także Ustawę z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Platforma Autenti może być także stosowana do przetwarzania dokumentów w procesach, dla których konieczne jest spełnienie wymogów Komisji Nadzoru Finansowego (w szczególności Komunikatu z dnia 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej).

3. Jakie dokumenty regulują usługi oferowane przez Autenti?

Autenti świadczy usługi zaufania na podstawie Polityki Świadczenia Usług Zaufania, która określa rodzaje, zasady i warunki ich świadczenia, zgodnie z Rozporządzeniem eIDAS, a także Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Autenti znajduje się na liście Niekwalifikowanych Dostawców Usług Zaufania prowadzonej przez Narodowy Bank Polski na zlecenie ministra właściwego ds. informatyzacji.

Dokumenty regulujące funkcjonowanie platformy Autenti oraz innych usług oferowanych przez spółkę Autenti można znaleźć na stronie internetowej autenti.com w zakładce "Regulaminy" lub bezpośrednio pod adresem <https://autenti.com/regulaminy/>. Znajdują się na niej m.in. Regulamin platformy Autenti, Polityka ochrony prywatności, Polityka Cookies czy Polityka świadczenia usług zaufania Autenti.

4. Co znaczy sformułowanie "zaufana strona trzecia"?

"Zaufaną stroną trzecią" (tzw. "TTP" z ang. Trusted Third Party) jest niezależny podmiot, który ułatwia interakcję między stronami, gwarantując bezstronność i obiektywne potwierdzenie wykonania określonych czynności faktycznych lub prawnych. Przykładem zaufanej strony trzeciej jest notariusz. Podobną rolę pełnią dostawcy usług

zaufania, którzy m.in. potwierdzają fakt podpisania określonego dokumentu, uwierzytelniania tożsamości osoby fizycznej czy walidacji podpisów elektronicznych.

W sytuacji, gdy podpis elektroniczny został złożony na platformie zaufanej strony trzeciej, potwierdzenie tej czynności w przyszłości i w pełni korzystanie ze skutków prawnych rozporządzenia eIDAS jest istotnie ułatwione. Autenti, działając jako zaufana strona trzecia, gwarantuje niezależne od wszystkich uczestników transakcji dowody z realizacji procesu złożenia podpisu elektronicznego.

5. Na jakiej podstawie Autenti staje się “zaufaną stroną trzecią”?

Autenti świadczy usługi zaufania na podstawie Polityki świadczenia usług zaufania, która określa rodzaje, zasady i warunki ich świadczenia.

6. Kto lub co potwierdza, iż Autenti jest usługą zaufania? Czy Autenti posiada wszystkie wymagane prawem zezwolenia lub koncesje?

Autenti Sp z o.o. została wpisana do rejestru niekwalifikowanych dostawców zaufania, prowadzonego przez Narodowy Bank Polski, dostępnego pod adresem: <https://www.nccert.pl/uslugiNK.htm>. Aby znaleźć się na takiej liście, dostawca usługi zaufania musi spełnić warunki określone rozporządzeniem eIDAS oraz Ustawą o usługach zaufania oraz identyfikacji elektronicznej. Dostawca usług zaufania działa w oparciu o udostępnioną politykę świadczenia usługi zaufania.

7. Jakie dowody otrzymują podpisujący dokumenty dzięki Autenti?

Podpisujący dokumenty otrzymują plik elektroniczny, spełniający wymogi trwałego nośnika, który zawiera podpisy elektroniczne stron. Do każdego dokumentu podpisanego za pośrednictwem platformy Autenti, dołączana jest Karta Podpisów.

Autenti gwarantuje, że podpisy elektroniczne zostały złożone pod dokumentem w jednakowym brzmieniu dla wszystkich stron. W tym celu, dokument przed złożeniem podpisów opatrywany jest kwalifikowaną pieczęcią elektroniczną (czyli zaawansowaną pieczęcią elektroniczną opartą na kwalifikowanym certyfikacie oraz kwalifikowanym elektronicznym znacznikiem czasu). Po złożeniu wszystkich podpisów, kwalifikowana pieczęć elektroniczna składana jest ponownie, w celu zabezpieczenia dokumentu i złożonych na nim podpisów przed jakimikolwiek, nieautoryzowanymi zmianami w przyszłości.

8. Dlaczego potwierdzenia Autenti są skutecznym dowodem?

Dokument podpisany podpisem elektronicznym, może stanowić dowód w postępowaniu sądowym, co gwarantuje art. 25 ust. 1 eIDAS, tj.: *“Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych.”*

Potwierdzenie podpisania określonego dokumentu wydane przez Autenti (w postaci Karty Podpisów czy Certyfikatu Autenti) stanowi dokument wydany przez zaufaną stronę trzecią, a jednocześnie dostawcę usług zaufania, który może zostać wykorzystany jako dowód w postępowaniu sądowym na okoliczność: podpisania dokumentu, jego treści, daty w jakiej podpisy zostały złożone. Co więcej, strony są w stanie wykazać, czy doszło do nieautoryzowanej i nieuprawnionej zmiany (przerobienia) danego dokumentu, czy zachowuje swoją integralność.

9. Czym jest podpis elektroniczny?

Podpis elektroniczny to deklaracja tożsamości autora, złożona w postaci elektronicznej pod dokumentem, na przykład imię i nazwisko, faksymile podpisu.

Zgodnie z prawem europejskim, podpis elektroniczny zawiera się w danych w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis (art. 3 pkt 10 Rozporządzenia eIDAS).

Podpisem elektronicznym jest zatem każdy rodzaj aktywności w świecie cyfrowym, z którym wiąże się pozostawienie danych identyfikujących autora – najczęściej poprzez określenie imienia i nazwiska. O ile podpisem elektronicznym jest każda deklaracja tożsamości złożona w postaci cyfrowej, to pewność podpisywania elektronicznego wzrasta, jeżeli ma miejsce w związku z usługami dostarczonymi przez wyspecjalizowanych dostawców usług zaufania.

10. Czym jest rozporządzenie eIDAS?

Jest to rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. UE. L. z 2014 r. Nr 257, str. 73). Rozporządzenie eIDAS gwarantuje jednolite traktowanie podpisów elektronicznych i dokumentu elektronicznego w całej Unii Europejskiej, zapewniając im rozpoznawalność i uznanie prawne. Na podstawie eIDAS wydana została polska Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2020 r. poz. 1173 z późn. zm.). Oba akty prawa regulują zasady funkcjonowania dostawców usług zaufania oraz świadczenia usług zaufania, a także ustanawiają ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego i usług certyfikacyjnych uwierzytelniania witryn internetowych.

11. Kiedy podpis elektroniczny na dokumentach jest ważny?

Podpis elektroniczny na dokumencie staje się ważny z momentem jego złożenia. Zgodnie z art. 61 §2 Kodeksu cywilnego: *“Oświadczenie woli wyrażone w postaci elektronicznej jest złożone innej osobie z chwilą, gdy wprowadzono je do środka komunikacji elektronicznej w taki sposób, żeby osoba ta mogła zapoznać się z jego treścią.”*

Zarówno krajowe, jak i europejskie prawo niekoniecznie wymaga, aby podpisy składane były zawsze na papierze oraz nie dyskryminuje czy odmawia ważności postaci elektronicznej. Zgodnie z prawem cywilnym: *“Z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej”* (art. 60 kodeksu cywilnego). Na uwagę zasługuje, że tylko nieliczne rodzaje dokumentów wymagają formy szczególnej, a nawet gdy wymagają takiej formy to jej niespełnienie nie zawsze powoduje nieważność danej czynności podpisywania. Warto też pamiętać, że nawet jeżeli dla ważności danej czynności konieczna jest forma pisemna to zastąpić ją można formą elektroniczną, składając pod dokumentem kwalifikowany podpis elektroniczny (por. 78 § 2 kodeksu cywilnego).

12. W jaki sposób Autenti zabezpiecza interesy podpisujących stron?

Autenti dba o interes stron, które podpisują Dokument, za pomocą zaawansowanych technologii informatycznych, w szczególności zabezpiecza integralność dokumentu zaawansowaną pieczęcią elektroniczną

opartą o kwalifikowany certyfikat, nanoszoną przed złożeniem podpisów przez strony oraz tuż po ich złożeniu. Dodatkowo Autenti umieszcza w dokumencie kwalifikowany znacznik czasu, który gwarantuje jednoznaczne określenie momentu sfinalizowania złożenia wszystkich wymaganych oświadczeń z datą pewną, mającą swoją prawną doniosłość. W ten sposób strony mają pewność, że dokument który podpisują, nie ulega nieautoryzowanym zmianom tuż po jego nadaniu i przeczytaniu, aż do momentu złożenia na nich podpisów, a także później, kiedy podpisy zostały już złożone. Każda ze stron ma dostęp do podpisanych dokumentów i może zweryfikować daty złożenia podpisów.

Dokumenty podpisywane za pośrednictwem platformy Autenti:

- są przechowywane w sposób bezpieczny,
- ich integralność jest zabezpieczona kwalifikowaną pieczęcią elektroniczną,
- są opatrzone kwalifikowanym znacznikiem czasu,
- są dostępne dla stron czynności prawnej w każdym czasie.

13. Czym jest Karta Podpisów Autenti?

Karta Podpisów to generowana w momencie nadania dokumentu do podpisu dodatkowa strona, dołączana do źródłowego pliku pdf, dzięki której można wykazać kto, kiedy i z jakiego urządzenia (IP) złożył podpis elektroniczny na dokumencie. Karta Podpisów obrazuje wszystkie dane, które zostały użyte do złożenia podpisu elektronicznego. Podpisy są zamieszczane chronologicznie.

Karta Podpisów zawiera w ramach wizualizacji, pola informujące o:

- rodzaju złożonego podpisu elektronicznego,
- imieniu i nazwisku podpisującego,
- adresie e-mail podpisującego,
- numerze telefonu podpisującego (opcjonalnie, w przypadku użycia dodatkowej metody identyfikacji podpisującego),
- danych dotyczących organizacji podpisującego i jego funkcji (opcjonalnie, w przypadku podpisywania dokumentu przez osobę reprezentującą wybraną organizację),
- rodzaju złożonego podpisu elektronicznego,
- zastosowanym uwierzytelnieniu podpisującego,
- powodzie złożenia podpisu,
- adresie IP uzyskanym z urządzenia podpisującego,
- dacie i godzinie złożenia podpisu.

Więcej informacji na temat Karty Podpisów znajdziesz pod adresem:

<https://autenti.com/karta-podpisow-czyli-zobaczyc-podpis-elektroniczny/>

14. Co to znaczy, że dokumenty podpisane elektronicznie przez Autenti są prawnie wiążące?

Oznacza to, że złożone podpisy elektroniczne oferowane przez Autenti posiadają swoje znaczenie prawne. Dokonanie czynności prawnej (złożenie oświadczenia woli) z użyciem podpisu elektronicznego oferowanego przez Autenti wywołuje skutki prawne i wiąże Strony danej czynności prawnej.

15. Czym jest gwarancja dostępności treści?

Autenti gwarantuje dostęp do dokumentów podpisanych za pośrednictwem platformy Autenti 24 godziny na dobę, 7 dni w tygodniu, z dowolnego urządzenia. Ponadto, po zakończeniu procesu podpisywania, podpisany dokument jest wysyłany drogą poczty elektronicznej (e-mail) do każdej z podpisujących stron. Można go zatem z łatwością zarchiwizować we własnych zasobach. Treść dokumentu dostępna jest dla podpisujących w postaci trwałego nośnika, a zatem zapewnia wypełnienie obowiązków jakie prawo nakłada na przedsiębiorców w umowach z konsumentami.

16. W jaki sposób gwarantowana jest niezmienność (integralność) treści?

Istotna dla podpisywania dokumentów elektronicznie jest integralność, czyli zapewnienie, że ich treść nie została w żaden sposób zmieniona od momentu nadania. Autenti gwarantuje integralność dokumentów przez użycie kwalifikowanych pieczęci elektronicznych. Pieczęć zabezpieczająca dokument po raz pierwszy jest składana w momencie wysłania dokumentu do podpisu, a po raz drugi, gdy wszystkie podpisy są już złożone. Dzięki pieczęci końcowej wiadomo, że wszystkie podpisy, które były konieczne do akceptacji dokumentu zostały zebrane, a wszelkie ewentualne dodatkowe podpisy nie były przedmiotem danego obiegu dokumentu na platformie Autenti. Każda z pieczęci jest uwidoczniona na Karcie Podpisu oraz zawiera dokładny czas jej nałożenia.

Zastosowane rozwiązanie umożliwia łatwe, natychmiastowe rozpoznanie czy w dokumencie pomiędzy czasem nałożenia pieczęci zabezpieczających przez Autenti wprowadzone zostały jakichkolwiek zmiany w treści dokumentu. Niezmienność dokumentu można zweryfikować samodzielnie np. za pomocą oprogramowania Adobe Acrobat Reader lub innego specjalistycznego weryfikatora podpisów i pieczęci elektronicznych.

17. Na czym polega znakowanie czasem dokumentów elektronicznych i jakie zastosowanie ma kwalifikowany elektroniczny znacznik czasu?

Znakowanie czasem dokumentów elektronicznych polega na wygenerowaniu przez usługę zaufania przy użyciu metod kryptograficznych elektronicznego potwierdzenia wiążącego dany dokument z datą.

Kwalifikowany elektroniczny znacznik czasu, który jest tworzony przez kwalifikowaną usługę zaufania, korzysta z prawnego skutku pewnej daty i czasu, jakie wskazuje, a włączenie go do dokumentu zapewnia logiczne połączenie czasu z momentem potwierdzenia jego treści przez wszystkich wymaganych podpisujących. Zarówno skutek prawny elektronicznego znacznika czasu, jak i jego dopuszczalność jako dowodu w postępowaniu sądowym, nie mogą być kwestionowane wyłącznie z tego powodu, że znacznik ten ma postać elektroniczną.

Dodatkowym elementem, który ułatwia interpretację ważności złożonych podpisów – i tym samym konserwację podpisu – jest stosowanie przez Autenti funkcjonalności LTV („Long Term Validation”), czyli dołączanie do podpisów odpowiedzi od systemów potwierdzających status certyfikatu podpisu elektronicznego. Umożliwia on skuteczne potwierdzenie tego, że certyfikat podpisującego był ważny w momencie jego składania.

18. Czym jest i na jakiej podstawie Autenti spełnia wymagania dotyczące trwałego nośnika?

Zgodnie z art. 2 pkt 4. Ustawy o prawach konsumenta, trwałe nośnik definiuje się jako: *“[...] materiał lub narzędzie umożliwiające konsumentowi lub przedsiębiorcy przechowywanie informacji kierowanych osobiście do niego, w sposób umożliwiający dostęp do informacji w przyszłości przez czas odpowiedni do celów, jakim te informacje służą, i które pozwalają na odtworzenie przechowywanych informacji w niezmienionej postaci”*. Dzięki rozwiązaniom technologicznym przyjętym przez Autenti dokumenty generowane po złożeniu podpisów i dostępne w ramach platformy Autenti, a także pliki wysyłane drogą poczty elektronicznej do podpisujących,

spełniają wymogi prawa przewidziane dla trwałych nośników i służą m.in. w zabezpieczeniu spełnienia obowiązku przedsiębiorców wobec osób działających na prawach konsumenta.

Więcej o trwałym nośniku przeczytasz pod adresem: <https://autenti.com/trwaly-nosnik/>

19. Czym jest i w jaki sposób gwarantowana jest autentyczność pochodzenia dokumentu oraz jego integralność?

Zabezpieczenie autentyczności i integralności treści dokumentu to podstawowa funkcjonalność wyróżniająca innowacyjną technologię Autenti od innych rozwiązań dostępnych na rynku. Podpisywanie na platformie Autenti odbywa się w ściśle zdefiniowanym procesie, w którym od momentu nadania dokumentu do zakończenia jego podpisywania przez wszystkie wymagane osoby jest on przechowywany i udostępniany upoważnionym osobom z użyciem zaawansowanych mechanizmów informatycznych. Zastosowane zabezpieczenia uniemożliwiają zmianę treści, która byłaby niezauważona. Dla potwierdzenia procesowego zabezpieczenia, Autenti stosuje pieczęci elektroniczne oparte o kwalifikowany certyfikat, które są składane na dokumencie natychmiast po jego nadaniu oraz po zakończeniu podpisywania i umożliwiają za pomocą dodatkowej warstwy wizualnej Karty Podpisów oraz technicznej pliku jednoznaczne określenie złożonych podpisów, bez zmiany dokumentu udostępnionego podpisującym. Stosowana pieczęć elektroniczna weryfikowana kwalifikowanym certyfikatem spełnia wymagania art. 36 eIDAS, w szczególności jest powiązana z dokumentem, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna w sposób automatyczny. Dla przykładu otwarcie dokumentu podpisanego w Autenti w aplikacji Adobe Acrobat Reader weryfikuje, czy nie dokonano zmian w opieczętowanym dokumencie, a w przypadku takich zmian wyraźnie o nich informuje. Każda dokument podpisany w Autenti dodatkowo jest oznaczony kwalifikowanym elektronicznym znacznikiem czasu, który nie tylko gwarantuje integralność dokumentu, ale zapewnia także korzystanie z domniemania dokładności daty i czasu, jakie wskazuje.

Dodatkowo, Autenti oferuje cyfrowy weryfikator plików – narzędzie umożliwiające weryfikację czy dany plik był podpisany na platformie Autenti.

20. Od czego zależy i jak wybrać właściwy rodzaj podpisu elektronicznego?

Rodzaj podpisu elektronicznego należy wybrać stosownie do formy czynności prawnej, jaka jest wymagana przepisami prawa dla jej ważności. Tylko dokumenty, które wymagają zachowania formy pisemnej pod rygorem nieważności (np. umowa przenosząca majątkowe prawa autorskie), muszą być podpisywane przy użyciu kwalifikowanego podpisu elektronicznego (forma elektroniczna). Zgodnie z Kodeksem cywilnym forma elektroniczna jest równoznaczna z formą pisemną. W innych przypadkach można z powodzeniem użyć innych rodzajów podpisu elektronicznego, jak e-podpis Autenti (forma dokumentowa).

21. Jakie są formy składania oświadczeń woli i do których mogę użyć podpisu elektronicznego?

Kodeks cywilny przewiduje:

- formę dokumentową (art. 772 Kodeksu cywilnego). Do jej zachowania wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie,
- zwykłą formę pisemną (art 78 Kodeksu cywilnego), tj. złożenie własnoręcznego podpisu na dokumencie;
- formę elektroniczną (art. 79 Kodeksu cywilnego), tj. złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym – jest ona równoważna formie pisemnej,
- formy szczególne, np. akt notarialny, notarialne poświadczenie podpisu.

Tylko w przypadkach ściśle zastrzeżonych przez przepisy prawa wymagane jest zachowanie formy pisemnej lub elektronicznej. Brak takiego zastrzeżenia pozwala na posługiwanie się dowolną formą, jednakże dla celów dowodowych pożądaną formą czynności prawnej jest forma dokumentowa – do której zastosowanie ma e-podpis Autenti.

22. Jaka jest różnica pomiędzy formą pisemną a dokumentową?

Formą pisemną jest własnoręczne złożenie podpisu. Formą elektroniczną jest złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym (podpis elektroniczny z użyciem kwalifikowanego certyfikatu). Forma elektroniczna jest równoważna formie pisemnej. Formą dokumentową jest złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie.

23. Które dokumenty mogę podpisywać podpisem elektronicznym (e-podpisem Autenti), a do których niezbędne będzie użycie kwalifikowanego podpisu elektronicznego (opcja także dostępna w ramach platformy Autenti)?

Podpisem elektronicznym można podpisać każdy dokument, dla którego przepisy prawa nie przewidują zachowania formy pisemnej pod rygorem nieważności lub formy szczególnej, takiej jak forma aktu notarialnego. Kwalifikowany podpis elektroniczny należy użyć jeżeli dla ważności danej czynności wymagany jest podpis własnoręczny bądź forma elektroniczna.

24. Czy mogę za pomocą platformy Autenti podpisywać dokumenty z osobami z zagranicy? Jak w takim przypadku będzie się miał do tego regulamin Autenti i przepisy prawa?

Autenti świadczy usługi zaufania w oparciu o Rozporządzenie eIDAS (Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. UE. L. z 2014 r. Nr 257, str. 73), które jest aktem prawa Europejskiego, stosowanym przez państwa członkowskie bezpośrednio. Podpisy oferowane przez Autenti mogą być zatem stosowane w całej Unii Europejskiej oraz w zależności od przypadku, również poza nią. Platforma Autenti oraz Regulamin Platformy Autenti są dostępne również w wersji angielskiej.

25. Jak weryfikowane są osoby podpisujące dokumenty na platformie Autenti?

Dane osobowe podpisujących pochodzą od nadawcy dokumentu. Co do zasady weryfikacja odbiorców leży po stronie nadawcy dokumentu, a rolą platformy Autenti jest umożliwienie, wskazanej przez nadawcę osobie, dostępu do dokumentu i możliwości złożenia podpisu, za pomocą różnych metod uwierzytelnienia lub zdalnej identyfikacji tożsamości. Podstawową daną, która jest weryfikowana jest adres e-mail. Należy pamiętać, aby dokumenty nadać na adres poczty elektronicznej, co do którego nadawca ma odpowiednią pewność, że jest adresem którym posługuje się osoba podpisująca. Dla zwiększenia poziomu bezpieczeństwa, w niektórych sytuacjach, zalecane jest stosowanie dodatkowych sposobów uwierzytelnienia, np. poprzez kod OTP (“one-time password”), który wysyłany jest SMSem pod numer telefonu odbiorcy. Bez jego użycia nie jest wówczas możliwe podpisanie dokumentu na platformie. Autenti oferuje również inne, dodatkowe metody potwierdzenia tożsamości osoby fizycznej na odległość, w ramach usługi BROKER.ID (ID Check & Liveliness, ID Check & Selfie, ID Check) lub możliwość skorzystania z kwalifikowanego podpisu elektronicznego.

26. W jaki sposób Autenti weryfikuje używane na platformie podpisy?

W Autenti, dzięki funkcjonalności "Weryfikator", można potwierdzić czy dokument był przetwarzany w ramach platformy Autenti, nie weryfikuje ona natomiast złożonych przez użytkowników podpisów. Walidacji podpisów można dokonać za pomocą publicznie dostępnych programów komputerowych (np. Adobe Acrobat Reader) lub serwisów internetowych. Najwyższą gwarancję poprawności walidacji dostarczają kwalifikowane usługi walidacji podpisów elektronicznych.

27. RODO a Autenti – czy następuje transfer danych osobowych poza Europejski Obszar Gospodarczy?

Dane osobowe związane ze świadczeniem usługi zaufania są zlokalizowane na terytorium Unii Europejskiej i nie są przesyłane do państw trzecich. Autenti korzysta natomiast z popularnych narzędzi analitycznych, jak również posiada profile w mediach społecznościowych, których serwery mogą znajdować się w państwie trzecim. O liście zaufanych partnerów przeczytasz w [Polityce Ochrony Prywatności](#) Autenti.

28. Kto może złożyć podpis elektroniczny?

Podpis na platformie Autenti może złożyć każda osoba fizyczna, zarówno w swoim imieniu, jak również działając w imieniu innej osoby fizycznej lub prawnej (w oparciu o stosowne pełnomocnictwo), posiadająca pełną zdolność do czynności prawnych. Do złożenia podpisu nie jest wymagane posiadanie konta na platformie Autenti.

29. Skąd wiadomo kto podpisał dokument?

Karta Podpisów Autenti zawiera wszystkie dane osób podpisujących, które zostały użyte do złożenia podpisów elektronicznych. Między innymi ich imię, nazwisko, adres e-mail, adres IP, dane firmy, którą reprezentują czy rodzaj e-podpisu, jaki użyli. Mogą się na niej pojawiać również informacje o dodatkowych metodach identyfikacji, dzięki którym dokonano weryfikacji tożsamości podpisującego lub dane pochodzące z kwalifikowanego certyfikatu podpisu elektronicznego, jeśli taki został użyty do złożenia podpisu. W celu dokonania dodatkowego uwierzytelnienia tożsamości podpisujących rekomendowane jest skorzystanie z usługi BROKER.ID, która wchodzi w skład ekosystemu usług Autenti.

30. Na jakiej podstawie Autenti przetwarza dane osobowe stron?

Autenti przetwarza dane osobowe swoich użytkowników jako Administrator Danych Osobowych, m.in. na podstawie art. 6 ust. 1 lit. b RODO. Przetwarzanie jest niezbędne dla celów wykonania zawartej umowy na świadczenie usług drogą elektroniczną. Dane zawarte w dokumentach przetwarzane są na podstawie powierzenia przetwarzania danych osobowych w relacji Autenti – użytkownik (odbiorca dokumentów). Więcej informacji w [Polityce Ochrony Prywatności](#) Autenti.

31. Dlaczego przechowywanie dokumentów podpisanych na platformie jest bezpieczne?

Dokumenty podpisane na platformie Autenti są przechowywane w sposób bezpieczny w środowisku chmurowym. Autenti stosuje georedundację plików oraz ich szyfrowanie, zarówno "at rest" jak i "in transit". Oznacza to, że dane przetwarzane za pośrednictwem platformy Autenti zabezpieczone są zarówno w trakcie ich przesyłu, jak i w trakcie ich przechowywania w chmurze. Każda wychodząca i przychodząca komunikacja HTTP jest zabezpieczona protokołem SSL, w standardzie nie niższym niż TLS 1.2. Komunikację HTTP zabezpieczają dodatkowo mechanizmy HTTP Strict Transport Security (HSTS) i Authenticated Origin Pulls, które utrudniają

podsywanie się pod usługę Autenti. Komunikacja email jest zabezpieczona kluczem DKIM oraz metodami SPF i DMARC w celu utrudnienia podszywania się pod usługę Autenti.

32. Kto korzysta z rozwiązań Autenti?

Na koniec 2020 roku z platformy Autenti korzystało ponad 1300 klientów i partnerów, którzy wykorzystywali platformę do celów komercyjnych, a ich liczba stale rośnie. Na liście podmiotów znajdują się liczne instytucje finansowe, w tym banki, firmy leasingowe, zakłady ubezpieczeń, ale także firmy produkcyjne i handlowe, firmy energetyczne, kancelarie prawne, uczelnie wyższe, organizacje publiczne czy organizacje pożytku publicznego. Wielu z nich Autenti prezentuje na swojej stronie internetowej, a wybrane studia przypadków na swoim blogu. Na życzenie rozmówców, przedstawiciele i eksperci Autenti odpowiedzą na indywidualne pytania.

33. Jaką infrastrukturę wykorzystuje Autenti do świadczenia usług?

Autenti do świadczenia usług korzysta z wyspecjalizowanych data center. Dostawcami kompleksowych rozwiązań technologicznych w zakresie przetwarzania danych są renomowani dostawcy usług przetwarzania danych w chmurze obliczeniowej, którzy gwarantują najwyższe standardy i bezpieczeństwo danych naszych klientów, legitymując się takimi certyfikatami jak: SOC I, SOC II, SOC III, ISO 2000:2011, ISO 22301:2012, ISO 27001:2013, ISO 27017:2015, ISO 27018:2014, ISO 27701, ISO 9001:2015. Autenti spełnia wymogi [komunikatu z dnia 23 stycznia 2020 r.](#), wydanego przez Urząd Komisji Nadzoru Finansowego, dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

34. Gdzie zlokalizowane są centra danych w których są zapisywane dokumenty podpisywane przez Autenti?

Centra danych, w których przetwarzane są dokumenty podpisywane przez Autenti znajdują się na terenie Unii Europejskiej, a więc w ramach Europejskiego Obszaru Gospodarczego oraz są odpowiednio chronione, aby dane przechowywane były w sposób bezpieczny.

35. Czy dokumentami podpisanymi elektronicznie można posługiwać się w sprawach sądowych?

Dokumenty podpisane elektronicznie mogą stanowić dowód w sprawie, co znajduje swoje odzwierciedlenie zarówno w polskich, jak i europejskich przepisach prawa. Zgodnie z art. 46 rozporządzenia eIDAS: *“Nie jest kwestionowany skutek prawny dokumentu elektronicznego ani jego dopuszczalność jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dokument ten ma postać elektroniczną”*. Zgodnie natomiast z art. 25 eIDAS: *“Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych.”*

36. Czy dokumenty podpisane elektronicznie mogą być wykorzystywane w relacjach międzynarodowych?

Dokumenty podpisywane za pośrednictwem platformy Autenti mogą być wykorzystywane w relacjach międzynarodowych. Bez wyjątków na terenie Unii Europejskiej, jak również poza nią – jeżeli porządek prawny danego kraju dopuszcza stosowanie podpisów elektronicznych, a dla danej czynności prawnej nie są określone szczegółowe wymagania ograniczające.

37. Jak długo przechowywane są dokumenty na platformie Autenti?

Czas przechowywania dokumentów na platformie Autenti jest uzależniony od umowy. Niezależnie od tego każdy podpisujący otrzymuje na trwałym nośniku podpisany dokument pocztą elektroniczną (e-mail) i może gromadzić w ten sposób podpisany dokument w swoim archiwum plików.

38. Kto ma dostęp do dokumentów podpisanych na platformie Autenti?

Do dokumentów podpisanych za pośrednictwem platformy Autenti mają dostęp jedynie osoby biorące udział w procesie podpisywania dokumentu, w tym osoby wskazane / upoważnione "do wglądu", złożenia komentarza, opinii czy parafki.

39. Jak dopasować treść dokumentów podpisywanych elektronicznie do tego trybu składania oświadczeń woli (przykłady)?

Dokumenty podpisywane podpisem elektronicznym przede wszystkim nie powinny zawierać takich postanowień jak:

- "Umowę sporządzono w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron" – plik elektroniczny nie ma tylko jednego lub dwóch egzemplarzy – może on być zwielowokrotniony, pod warunkiem, że nie zostanie naruszona integralność dokumentu. Integralność dokumentu można sprawdzić poprzez jego walidację w takich narzędziach jak np. Adobe Acrobat Reader;
- "Umowa zawarta w Krakowie" – podpisując elektronicznie, nie ma określonego miejsca zawarcia umowy;
- "Zmiana umowy może nastąpić w formie pisemnej pod rygorem nieważności" – stosując tę klauzulę, można zamknąć sobie drogę do zmiany treści dokumentu w formie dokumentowej, bowiem zmianę jej treści wszystkie strony będą musiały potwierdzić na piśmie bądź cyfrowo – wyłącznie z użyciem kwalifikowanego podpisu elektronicznego.

Zalecamy natomiast, aby dodawać takie zapisy jak np.:

- "Umowa została zawarta z dniem złożenia podpisu elektronicznego przez ostatnią ze Stron" lub wskazanie konkretnej daty zawarcia umowy, której zawarcie będzie potwierdzane podpisami elektronicznymi ;
- "Umowa została zawarta z wykorzystaniem podpisów elektronicznych Stron";
- Zawarcie w treści dokumentu właściwego dla stron adresu e-mail i numeru telefonu poszczególnych podpisujących.

40. W jaki sposób Autenti zarządza incydentami bezpieczeństwa?

W Autenti wdrożona jest procedura zarządzania incydentami bezpieczeństwa oraz naruszeniami. Prowadzony jest również stosowny rejestr incydentów i naruszeń. Dokumentacja podlega corocznemu audytowi i aktualizacji.

41. Jakie procedury Autenti stosuje w zakresie zarządzania ryzykiem bezpieczeństwa informacji?

W Autenti wdrożone są procedury bezpieczeństwa i ochrony danych osobowych, zgodne z takimi normami jak ISO 27001:2017. Nad ich zgodnością oraz realizacją czuwa Compliance Officer oraz Inspektor Ochrony Danych. Przykładowo są to: "Polityka bezpieczeństwa informacji i ochrony danych", "Instrukcja zarządzania bezpieczeństwem informacji Autenti Trust Center", "Instrukcja zarządzania infrastrukturą IT".

42. Czy Autenti posiada stosowne ubezpieczenie odpowiedzialności cywilnej (OC)?

Tak, Autenti posiada stosowne ubezpieczenie OC na kwotę 5 000 000 zł.

43. Czy Autenti wprowadziło i utrzymuje polityki / procedury mające na celu przeciwdziałanie praniu pieniędzy, finansowaniu terroryzmu, łapownictwu i korupcji?

Tak. Autenti przestrzega polityk mających na celu przeciwdziałanie praniu pieniędzy, finansowaniu terroryzmu, łapownictwu i korupcji.

44. Jak Autenti realizuje zobowiązanie do zachowania w tajemnicy Informacji Poufnych?

Treść dokumentów procesowanych lub przechowywanych przez Autenti jest należycie szyfrowana, a dostęp do narzędzi i systemów z danymi użytkowników posiadają nieliczne osoby pracujące nad zapewnieniem właściwego poziomu ich bezpieczeństwa, które posiadają stosowne upoważnienie. Wszyscy pracownicy, współpracownicy oraz podwykonawcy Autenti są zobowiązani na piśmie do zachowania poufności. Autenti dba o systematyczne podnoszenie świadomości swoich pracowników w tym zakresie, jak również wdraża odpowiednie środki organizacyjne i techniczne.

W Autenti powołano osobę pełniącą funkcję Inspektora Ochrony Danych Osobowych, odpowiedzialną za monitorowanie przestrzegania właściwych przepisów prawa. Inspektor aktywnie uczestniczy w kształtowaniu polityki ochrony danych w Autenti oraz odpowiednich środków technicznych i organizacyjnych dla najpełniejszej ochrony poufności danych.

45. Jak wyglądają procedury BCP w Autenti?

W Autenti został opracowany, wdrożony i zakomunikowany Plan Ciągłości Działania (BCP) oraz inne procedury mające na celu zapewnienie nieprzerwanego świadczenia usług.

46. Jak Autenti realizuje usługi wsparcia technicznego i SLA?

Autenti oferuje swoim Klientom wsparcie techniczne oraz SLA. Standardowo oferowana jest dostępność platformy Autenti na poziomie 97% oraz wsparcie techniczne od poniedziałku do piątku w godzinach od 9:00 do 17:00, a wyższy poziom jest dostępny na indywidualnych warunkach.

47. Czy Autenti działa zgodnie z normami PN- ISO/IEC ISO 20000, PN -EN ISO/IEC 27001, PN-EN ISO 22301; ISO/IEC 27017 lub ISO/IEC 27018?

Autenti działa w oparciu o normę PN-EN ISO/IEC 27001:2017 oraz inne najlepsze i powszechnie stosowane praktyki bezpieczeństwa. Ponadto, usługodawcy, z których usług korzysta Autenti, gwarantują najwyższą jakość usług oraz zgodność z takimi normami jak ISO/IEC 27001:2017, ISO 20000, ISO/IEC 23001, ISO/IEC 27017, ISO/IEC 27018 czy SOC 1 i SOC 2.

48. Czy Autenti gwarantuje bezpieczeństwo sieci w ramach swojej działalności?

Autenti w trybie ciągłym zarządza bezpieczeństwem sieci komputerowej, która stanowi część infrastruktury świadczenia usług zaufania. Nadzór nad siecią wewnętrzną pełnią wyznaczeni i wyspecjalizowani do tego administratorzy Autenti Trust Center, odpowiedzialni za zapewnienie i monitorowanie wysokiego poziomu bezpieczeństwa. Sieć wewnętrzna jest poddawana regularnym testom bezpieczeństwa oraz analizie podatności.

Wprowadzone zostały m.in. takie zabezpieczenia jak kontrola dostępu oraz segmentacja sieci. W rozwiązaniach klasy Enterprise, na żądanie klientów Autenti umożliwia dostęp do komunikacji z siecią Autenti za pomocą dedykowanych, prywatnych tuneli VPN.

49. Jakie testy penetracyjne wykonuje Autenti?

Autenti wykonuje okresowe testy penetracyjne w oparciu o metodologię OWASP TOP10 i OWASP ASVS 3.01.