



## Polski System Oceny Zgodności Oprogramowania

---

**Status:** Wersja opublikowana

**Nazwa pliku:** System Oceny Zgodności  
Oprogramowania - v\_1\_0

**Ostatnia modyfikacja:** 2008-11-27 14:40:00

**Autor:** Członkowie Stowarzyszenia na rzecz Atestacji i  
Standaryzacji Oprogramowania

---

Poprzednia wersja:

**Status:** Wersja recenzowana

**Nazwa pliku:** System Oceny Zgodności  
Oprogramowania - v\_0\_5

**Ostatnia modyfikacja:** 2008-07-08 11:15:00

**Etap:** Zatwierdzenie

**Autor:** Członkowie Stowarzyszenia na rzecz Atestacji i  
Standaryzacji Oprogramowania

---

Zakres zmian:

- Poprawki naniesione w procesie przeglądu końcowego.

## Spis treści

<b>1.</b>	<b>Wstęp i odwołania .....</b>	<b>3</b>
1.1.	Wstęp.....	3
1.2.	Cel ustanowienia standardu .....	3
1.3.	Odniesienie do modelu jakości .....	3
1.4.	Słownik pojęć.....	6
<b>2.</b>	<b>Własność Systemu Oceny Zgodności Oprogramowania .....</b>	<b>8</b>
2.1.	Własność Systemu .....	8
2.2.	Proces ewaluacji i nadzoru .....	8
2.3.	Konteksty użycia .....	9
2.4.	Porządek prawny.....	10
<b>3.</b>	<b>Wymagania dotyczące zgodności w obszarze E .....</b>	<b>11</b>
3.1.	Opis certyfikatu .....	11
3.2.	Symbol certyfikatu.....	11
3.3.	Poziomy certyfikacji .....	11
3.4.	Wymagania szczegółowe .....	11
3.4.1.	Poziom podstawowy .....	12
3.5.	Wymagania szczegółowe dotyczące ewaluacji .....	12
<b>4.</b>	<b>Wymagania dotyczące zgodności w obszarze S .....</b>	<b>14</b>
4.1.	Opis certyfikatu .....	14
4.2.	Symbol certyfikatu.....	14
4.3.	Poziomy certyfikacji .....	14
4.4.	Wymagania szczegółowe .....	15
4.4.1.	Poziom podstawowy .....	15
4.5.	Wymagania szczegółowe dotyczące ewaluacji .....	16
<b>5.</b>	<b>Wymagania dotyczące zgodności w obszarze § .....</b>	<b>17</b>
5.1.	Opis certyfikatu .....	17
5.2.	Symbol certyfikatu.....	17
5.3.	Poziomy certyfikacji .....	17
5.4.	Wymagania szczegółowe .....	18
5.4.1.	Poziom podstawowy .....	18
5.5.	Wymagania szczegółowe dotyczące ewaluacji .....	19
<b>6.</b>	<b>Wzór deklaracji zgodności dla certyfikatu E .....</b>	<b>20</b>
<b>7.</b>	<b>Wzór deklaracji zgodności dla certyfikatu S .....</b>	<b>21</b>
<b>8.</b>	<b>Wzór deklaracji zgodności dla certyfikatu § .....</b>	<b>22</b>
<b>9.</b>	<b>Odnośniki .....</b>	<b>23</b>

## **1. Wstęp i odwołania**

### **1.1. Wstęp**

Niniejszy dokument powstał w wyniku prac Polskiego Stowarzyszenia na rzecz Badań i Atestacji Oprogramowania, a jego celem jest określenie zasad nadawania wspólnych znaków towarowych produktom softwareowym, zwanych Certyfikatami Zgodności (Certyfikatami Jakości).

Jakość oprogramowania jako produktu jest przedmiotem badań od czasu sformułowania pojęcia inżynierii oprogramowania i choć pierwsze modele jakości (McCall<sup>1</sup> i Boehm<sup>2</sup>) powstały pod koniec lat 1970, to praktycznie żaden z nich, ani żaden z modeli opracowanych w kolejnych latach nie stał się standardem w rozumieniu rynku IT. Model jakości, rozumiany jako sposób (język) opisu, stanowi również język używany w niniejszym dokumencie do wyrażenia wymogów jakościowych stawianych oprogramowaniu w Polskim Systemie Zgodności Oprogramowania. Jako model jakości w dokumencie stosowany jest model rozwijany przez ISO/IEC JTC1/SC7 pod nazwą SQuaRE<sup>3</sup> (Software Product Quality Requirements and Evaluation). Dalsze informacje na temat modelu jakości znajdują się w rozdziale 1.

Właścicielem niniejszego Systemu Oceny Zgodności Oprogramowania są Członkowie zrzeszeni w SASO reprezentowani przez organy wymienione w Statucie SASO. W zakresie stosowania Systemu Oceny Zgodności Oprogramowania zostanie powołana Rada jednostek certyfikujących, która będzie wyrażała swój głos w obszarze ewaluacji oprogramowania i zasad stosowania niniejszego Systemu.

Członkowie i Zarząd SASO mają nadzieję, że opublikowanie niniejszego standardu wzbogaci rynek o możliwość wyrażania jakości oprogramowania w formie czytelnej dla Klientów i Użytkowników, oraz zachęci samych Producentów do inwestowania w jakość swoich produktów, jako w istotny element przewagi konkurencyjnej na rynku.

### **1.2. Cel ustanowienia standardu**

Brak standardów oceny jakości oprogramowania pozbawia Odbiorców obiektywnych narzędzi umożliwiających ocenę jakości oprogramowania. Brak standardów oznacza brak niezależnych podmiotów dokonujących badań oprogramowania i przekazujących obiektywne informacje dla odbiorców IT. W konsekwencji Producenci oprogramowania inwestują środki w doskonalenie procesów i certyfikację metod organizacji przedsiębiorstwa nie traktując jakości produktu jako potencjalnego źródła przewagi konkurencyjnej. Efektem takiego stanu rzeczy są produkty nie odpowiadające potrzebom ich nabywców, lub realizujące zadania w sposób nie dający użytkownikom korzyści w stosunku do sytuacji pracy ręcznej.

Producenci oprogramowania działając na wysoce konkurencyjnym rynku starają się dopasowywać swoje koszty do wymogów wynikających z oferty konkurencji i czynników jakimi kierują się Klienci przy wyborze

oprogramowania. Ponieważ użytkownicy rzadko mają możliwość oceny jakości oprogramowania przed zakupem i nie mając kryteriów porównania jakości pomiędzy produktami często sami nie przywiązują dużej wagi do czynników jakościowych.

Ustanowienie niniejszego standardu ma na celu dostarczenie Klientom i Użytkownikom obiektywnego narzędzia do porównywania jakości produktów, a z drugiej strony narzędzia dla Producentów do manifestowania swojej dbałości o jakość produktu IT. Twórcy zakładają, że Producenci mając do dyspozycji niniejszy standard sami rozpoczną inwestycje w jakość, jako w istotny element przewag konkurencyjnej na rynku IT, co wpłynie pozytywnie na końcową jakość produktów dostępnych na rynku i w konsekwencji na wzrost opłacalności inwestowania w rozwiązania IT.

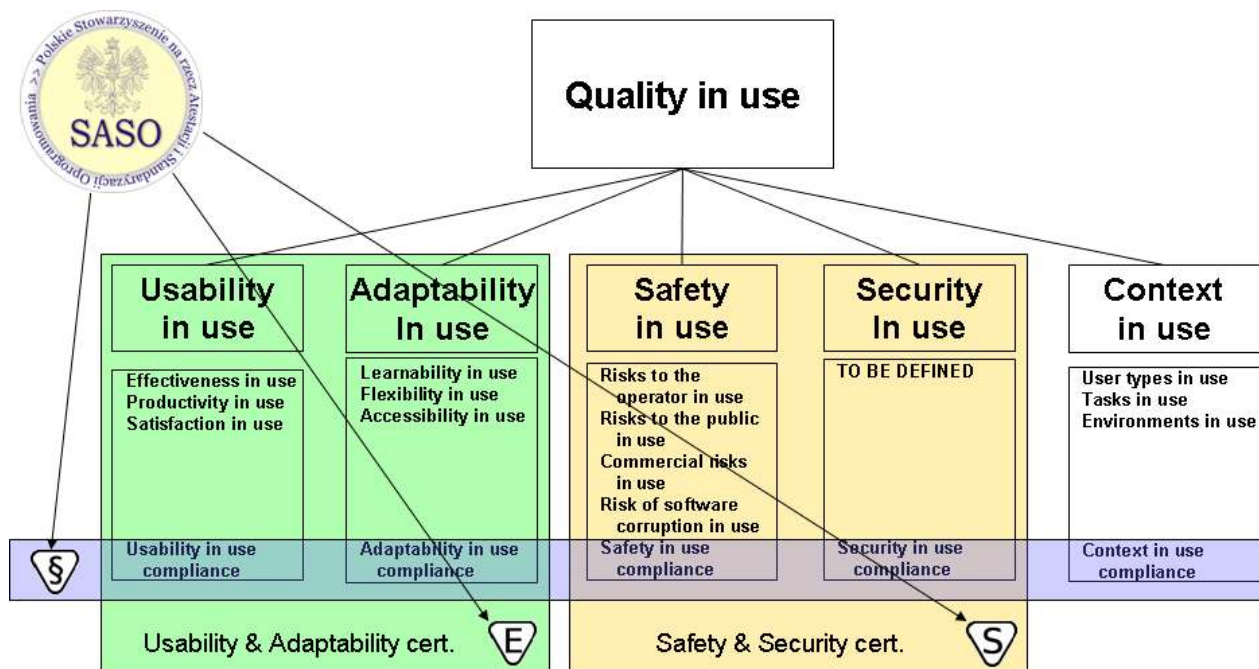
### 1.3. Odniesienie do modelu jakości

Językiem opisu jakości przyjętym w niniejszym dokumencie jest model SQuaRE rozwijany przez komitet ISO/IEC JTC1/SC7 i publikowany w serii norm ISO/IEC 25000. Model ten czerpie z doświadczeń zgromadzonych przez badaczy na przestrzeni ostatnich 40 lat formułując pojęcia, charakterystyki i podcharakterystyki zarówno z perspektywy użytkownika (Software Quality in Use), jak również pozwalając dekomponować te wymagania na definicje jakości technicznej-dynamicznej (External Software Quality) i jakości technicznej-statycznej (Internal Software Quality). Ponieważ niniejszy System ma w zamierzeniu być językiem komunikacji Klientów z Producentami IT wybrano perspektywę użytkownika jako podstawę terminologiczną.

Niniejszy System definiuje 3 obszary badania zgodności:

- Zgodność w obszarze ergonomii opisana w rozdziale 3
- Zgodność w obszarze bezpieczeństwa opisana w rozdziale 4
- Zgodność w obszarze wymagań formalnych opisana w rozdziale 5

Odniesienie obszarów oceny zgodności do modelu jakości przedstawia rysunek 1.



Rys. 1. - Odniesienie obszarów oceny zgodności do modelu SQaRE na podst. ISO/IEC 25010 CD z 2007<sup>1</sup>

Szczegółowe rozwinięcie wymogów w poszczególnych obszarach przedstawione jest w kolejnych rozdziałach.



## 1.4. Słownik pojęć

<b>SASO</b>	Polskie Stowarzyszenie na rzecz Atestacji i Standaryzacji Oprogramowania.
<b>Jednostka Certyfikująca</b>	Podmiot upoważniony na mocy podpisanej umowy z SASO, do nadawania Certyfikatu zgodności po przeprowadzeniu procedury ewaluacji opisanej w niniejszym dokumencie.
<b>Rada Jednostek Certyfikujących</b>	Ciało powołane do zarządzania procesem certyfikacji składające się z przedstawicieli Jednostek certyfikujących. Do czasu powołania Rady składającej się z minimum pięciu Jednostek Certyfikujących obowiązki Rady wykonuje Zarząd SASO.
<b>Certyfikat zgodności</b>	Dokument wydawany przez Jednostkę certyfikującym zgodnie z jej uprawnieniami i niniejszym Systemem Oceny Zgodności Oprogramowania określający prawo do posługiwania się Znakiem jakości.
<b>Znak jakości</b>	Jest to zarejestrowany znak towarowy, którym zarządza SASO zgodnie z niniejszym Systemem Oceny Zgodności Oprogramowania oraz Statutem.
<b>Znak towarowy</b>	Znak zarejestrowany w Urzędzie Patentowym Rzeczypospolitej Polskiej zgodnie z ustawą o ochronie własności przemysłowej (DzU 2003 nr 119 poz 1117).
<b>Nadanie certyfikatu</b>	Udzielenie przez SASO, za pośrednictwem Jednostki Certyfikującej niewyłącznej licencji na posługiwanie się określonym znakiem towarowym zgodnie z niniejszym Systemem Oceny Zgodności Oprogramowania.
<b>Ewaluacja</b>	Proces badania zgodności oprogramowania przeprowadzony przez Jednostkę Certyfikującą zgodnie z treścią niniejszego dokumentu
<b>Zgłaszający</b>	Jednostka zgłaszająca produkt do ewaluacji, podpisująca umowę z Jednostką Certyfikującą, określająca zakres ewaluacji, zakres stosowalności.
<b>Polityka bezpieczeństwa<sup>5</sup></b>	(ang. security policy) jest zbiorem spójnych, precyzyjnych i zgodnych zobowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Określa ona, które zasoby i w jaki sposób mają być chronione.
<b>Profil bezpieczeństwa</b>	Opisuje wymagania bezpieczeństwa zdefiniowane dla wybranego obszaru systemu lub części oprogramowania. Wymagania zdefiniowane są oddzielnie dla Oprogramowania oraz dla środowiska, w którym

Oprogramowanie pracuje lub będzie docelowo pracować. Profil bezpieczeństwa abstrahuje od sposobu implementacji poszczególnych wymagań.



## **2. Własność Systemu Oceny Zgodności Oprogramowania**

### **2.1. Własność Systemu**

Właścicielem niniejszego Systemu Oceny Zgodności Oprogramowania są Członkowie zrzeszeni w SASO reprezentowani przez organy wymienione w Statucie SASO. Właściciele udzielają publicznej, niewyłącznej licencji do korzystania z niniejszego dokumentu wszystkim zainteresowanym. W przypadku powielania całości lub części treści niniejszego dokumentu wymagane jest podanie odniesienia:

*Polskie Stowarzyszenie na rzecz Atestacji i Standaryzacji Oprogramowania, Polski System Oceny Zgodności Oprogramowania, <http://www.saso.org.pl>, SASO, Poznań 2008*

System Oceny Zgodności Oprogramowania składa się z dwóch obszarów: wymagań dla oprogramowania jako produktu oraz wymagań dla procesu ewaluacji. System powstaje i jest modyfikowany na wniosek Członków SASO, natomiast w obszarze wymagań dla procesu ewaluacji wnioskującym o zmianę może być Rada Jednostek Certyfikujących, która również bierze udział w pracach nad tą częścią Systemu.

Niniejszy dokument w najnowszej wersji, oraz regulamin znaków jakości oprogramowania opublikowane są pod adresami: <http://www.saso.org.pl/images/dokumenty/sozo.pdf>, <http://www.saso.org.pl/images/dokumenty/regulamin.pdf>.

### **2.2. Proces ewaluacji i nadzoru**

Proces ewaluacji przebiega zgodnie z § 5 regulaminu znaków jakości i składa się z następujących etapów:

- 1) Podmiot zainteresowany certyfikacją (Zgłaszający) występuje do Jednostki Certyfikującej z informacją o oprogramowaniu, które chce poddać certyfikacji, z informacją o tym o jaki znak się ubiega i na jakim poziomie certyfikacji. Do zgłoszenia załącza deklarację zgodności określającą biznesowe konteksty użycia aplikacji.
- 2) Jednostka certyfikująca powiadamia SASO o zgłoszeniu, a dla Zgłaszającego określa jakie dokumenty i materiały powinny zostać dostarczone celem wykonania certyfikacji oraz określa warunki finansowe certyfikacji.
- 3) Zgłaszający dostarcza wymagane materiały i wniosek o certyfikację.
- 4) Jednostka certyfikująca wykonuje certyfikację adekwatnie do zaplanowanych badań wynikających z rodzaju aplikacji i deklaracji zgodności, oraz wymaganego poziomu certyfikacji.
- 5) Jednostka certyfikująca podejmuje decyzje o wydaniu certyfikatu lub odmowie wydania certyfikatu.
- 6) Jednostka certyfikująca informuje SASO o wydaniu lub odmowie wydania certyfikatu. SASO udostępnia publicznie informacje o wydanych certyfikatach, a dodatkowo Jednostkom certyfikującym przekazuje informację o odmowach wydania certyfikatu.



Po wydaniu certyfikatu Jednostka Certyfikująca sprawuje nadzór nad produktem badając, czy nie mają miejsca zmiany wersji aplikacji i opatrywania znakiem jakości innej wersji niż ta, dla której wydano certyfikat, badaniem czy nie zachodzą zmiany w deklaracji zgodności zmieniające interpretację obszarów zastosowań aplikacji. Nadzór odbywa się zgodnie z umową zawartą pomiędzy Jednostką Certyfikującą i Zgłaszającym.

Istotnym elementem badania oprogramowania uruchomionego na rzeczywistym środowisku jest dostęp do danych zgromadzonych w systemie. W tym przypadku Jednostka Certyfikująca musi posiadać uprawnienia szczegółowe do wykonania danej ewaluacji, oraz zakres jej umowy z SASO musi dopuszczać ewaluację na systemach uruchomionych produkcyjnie.

Jednostki Certyfikujące dokonujące certyfikacji produktów mające dostęp do tajemnicy przedsiębiorstwa Zgłaszającego zobowiązane są do odpowiedniego zabezpieczenia danych Zgłaszającego, oraz zawarcie z SASO w umowie zobowiązań do stosowania systemu ochrony danych Zgłaszających oraz odpowiednich klauzul w umowach ze Zgłaszającym.

### 2.3. Konteksty użycia

Biznesowe konteksty użycia aplikacji implikują szczegółowe wymagania dodatkowe dla poszczególnych obszarów zastosowania. Każdy obszar definiuje wymagania jakie należy dopisać do wymagań podstawowych (zdefiniowanych w niniejszym dokumencie) dla każdego znaku jakości z rozróżnieniem poziomów certyfikacji. Aktualne wymagania dla poszczególnych obszarów biznesowych publikowane są na stronie SASO.

W przypadku wystąpienia Zgłaszającego o certyfikację dla nowego kontekstu użycia następuje uzgodnienie pomiędzy Jednostką Certyfikującą a SASO jednostki, która przygotowuje propozycję treści wymagań dla tego kontekstu użycia. Przygotowane wymagania szczegółowe rozsyłane są do akceptacji członkom SASO, Jednostkom Certyfikującym i innym podmiotom współpracującym z SASO. W sytuacji nie zgłoszenia krytycznych zastrzeżeń w ciągu 3 tygodni od dnia rozesłania wymagań szczegółowych lub w przypadku osiągnięcia wcześniej zgody na proponowaną treść wymagań szczegółowych następuje zatwierdzenie wymagań i opublikowanie ich na stronie SASO. Od tego momentu wymagania stają się obowiązujące dla nowego kontekstu użycia i stają się częścią warunków uzyskania certyfikatu przez Zgłaszającego, który wystąpił o certyfikację dla tego obszaru.

W sytuacji kiedy Jednostka Certyfikująca, Komitet Techniczny ds. Systemu Oceny Zgodności Oprogramowania SASO lub inny podmiot za pośrednictwem Członka SASO zgłosi potrzebę zmiany wymagań szczegółowych zawartych w niniejszym dokumencie lub wymagań szczegółowych dla konkretnego kontekstu użycia następuje procedura zbliżona do opracowania nowych wymagań. SASO ustala podmiot, który przygotowuje nową propozycję treści wymagań, która następnie jest rozsyłana do akceptacji analogicznej jak w przypadku nowych wymagań.

Przygotowujący wymagania szczegółowe dla poszczególnych poziomów certyfikacji każdego ze znaków należy kierować się poziomem ryzyka związanym z certyfikacją uwzględniając specyfikę biznesowego kontekstu użycia:

Poziom podstawowy	występują nieznaczne ryzyka zauważalne w czasie użycia aplikacji
Poziom ★★	występują nieznaczne ryzyka wyłącznie dla wadliwego użycia aplikacji na poziomie działającej aplikacji
Poziom ★★★	nie występują ryzyka zauważalne na poziomie działającej aplikacji
Poziom ★★★★	występują nieznaczne ryzyka zauważalne na poziomie projektu, kodu źródłowego, ale nie na poziomie działającej aplikacji
Poziom ★★★★★	nie występują jakiegokolwiek ryzyka w zakresie projektu, kodu źródłowego i działającej aplikacji

Dla nowego biznesowego kontekstu użycia dokonuje się analizy cech aplikacji, które mogą wносить ryzyka użycia.

## 2.4. Porządek prawny

Pomiędzy SASO a Jednostką Certyfikującą zawierana jest umowa o udzielenie prawa licencyjnego do nadawania Znaków Jakości. Umowa określa warunki na jakich Jednostka Certyfikująca może przeprowadzać badania i wydawać certyfikaty.

Przed zawarciem umowy Jednostka Certyfikująca potwierdza spełnienie wymagań szczegółowych związanych z ewaluacją w każdym z obszarów certyfikacji oraz prowadzenie procesu ewaluacji zgodnie z normą ISO/IEC 25040 (ISO/IEC 14598-5). SASO prowadzi nadzór nad procesem ewaluacji poprzez prawo do audytu dokumentów ewaluacyjnych nie objętych tajemnicami przedsiębiorstw, w szczególności:

- a) treści zgłoszeń od Zgłaszających
- b) przeglądu deklaracji zgodności, dokumentacji użytkowej
- c) przeglądu planów ewaluacji
- d) przeglądu raportów z ewaluacji
- e) przeglądu raportów z wykonania czynności nadzoru

Zgłaszający zawiera umowę o wykonanie badania i nadzoru certyfikującego z Jednostką Certyfikującą, która informuje SASO o wydanych, zawieszonych i cofniętych certyfikatach celem publikowania tej informacji na stronach SASO.

### **3. Wymagania dotyczące zgodności w obszarze E**

#### **3.1. Opis certyfikatu**

Certyfikat zgodności E wydawany jest dla obszaru Ergonomii i Efektywności, a obejmuje charakterystyki modelu SQuaRE: Użyteczność (Usability in use), Dostosowalność (Adaptability in use). Certyfikat stosowany jest dla określonych w Deklaracji Zgodności obszarów zastosowania. Wymagane jest aby w instrukcji użytkownika lub na stronie producenta widniała szczegółowa informacja na temat obszarów zastosowania produktu, dla której wydano certyfikat zgodności oraz informacje o tym jaka była konfiguracja sprzętowa, na której wykonano pomiary efektywności.

#### **3.2. Symbol certyfikatu**

Nadanie certyfikatu wiąże się z przyznaniem prawa do stosowania dla konkretnego numeru wersji znaku towarowego E, który zaprezentowany jest na rysunku 2.



Rys. 2. - Znak potwierdzający zgodność w obszarze ergonomii

Przy znaku podaje się poziom certyfikacji (patrz rozdział 3.3), dokładny numer wersji oraz informacje o miejscu w którym można zapoznać się z deklaracją zgodności specyfikującą biznesowe konteksty użycia, oraz parametrami środowiska na którym badano efektywność oprogramowania.

#### **3.3. Poziomy certyfikacji**

Obszar certyfikacji obejmuje charakterystyki Użyteczność (Usability in use), Dostosowalność (Adaptability in use). Dla każdej z charakterystyk zdefiniowano pod-charakterystyki, konkretne miary i ich oczekiwane wartości. Przyznanie produktowi odpowiedniego poziomu certyfikatu wiąże się z poświadczeniem przez Jednostkę Certyfikującą spełnienia wszystkich wymogów dla danego poziomu (w sytuacji kiedy wynik choćby jednego pomiaru nie spełnia wymagań minimalnych określony poziom certyfikacji nie może być przyznany).

#### **3.4. Wymagania szczegółowe**

W niniejszym rozdziale opisano podstawowe wymogi dla wszystkich obszarów zastosowań. W przypadku określenia w deklaracji kontekstów użycia, należy uzupełnić zestaw mierzonych parametrów o parametry wynikające z danego kontekstu użycia. W przypadku braku określenia miar dla wskazanego kontekstu użycia Jednostka Certyfikująca wspólnie ze Zgłaszającym oraz Radą Jednostek Certyfikujących dokonuje analizy ryzyk

związanych ze stosowaniem produktu dla tego kontekstu użycia publikując wymagania na stronach SASO zgodnie z procedurą opisaną w rozdziale 2.3.

### 3.4.1. Poziom podstawowy

<b>Wymaganie</b>	<b>Wymagana cecha (miara)</b>	<b>Odniesienie do modelu</b>
Oprogramowanie nie zmusza użytkownika do oczekiwania	Wszystkie ekrany/raporty wywoływane w celu wykonania na nich jakichś czynności pojawiają się szybko (szybkość jest zależna od częstotliwości użycia). Łączny czas przestoju w wyniku oczekiwania na reakcje oprogramowania przy typowym sposobie użytkowania nie przekracza 30 minut na 8 godzin pracy.	Usability in use / Effectiveness
Użytkownik pracując z oprogramowaniem szybko realizuje zadania	Oprogramowanie jest skonstruowane w taki sposób, że wykonanie każdej czynności (rozumie się przez to wszystkie zadania w oprogramowaniu jakie należy wykonać aby zrealizować zadanie) przez przeszkolonego użytkownika zajmuje mniej czasu niż wykonanie tego samego zadania w alternatywny sposób (bez użycia oprogramowania).	Usability in use / Productivity
Oprogramowanie jest przyjazne i wspiera użytkownika	Oprogramowanie zawiera rozwiązania ułatwiające użytkownikowi realizację zadania, w szczególności takie, które umożliwiają wykorzystanie raz wprowadzonych informacji, weryfikują wystąpienie prostych błędów w danych wprowadzanych przez użytkownika i podpowiadają co należy wykonać.	Usability in use / Satisfaction
Oprogramowanie jest łatwe do nauczenia oraz do ponownego nauczenia po okresie nie używania (jest intuicyjne)	Przeszkolenie użytkownika w zakresie używania oprogramowania nie zajmuje więcej czasu niż przeszkolenie użytkownika w sytuacji gdyby czynności były realizowane bez oprogramowania. Oprogramowanie posiada wbudowane i łatwe do odnalezienia wyjaśnienia dla użytkownika opisujące sposób w jaki realizuje się poszczególne zadania.	Adaptability in use / Learnability
Oprogramowanie jest zgodne z wymaganiami formalnymi dla szybkości pracy i łatwości dostosowania, o ile takie występują	W przypadku oprogramowania użytkowanego przez określone grupy użytkowników (np. z ograniczeniami ruchowymi i percepcyjnymi) lub w określonych miejscach (np. miejsca o dużym natężeniu światła i dźwięku) oprogramowanie spełnia wymagania formalne dla takich sposobów użycia.	Usability in use, Adaptability in use / Compliance

Tab. 1. - *Wymagania szczegółowe dla certyfikacji E*

### 3.5. Wymagania szczegółowe dotyczące ewaluacji

Proces ewaluacji jest ściśle związany z wymaganiami wynikającymi z deklarowanych kontekstów użycia oraz z parametrami technicznymi systemu w ramach którego będzie uruchamiane oprogramowanie. Ewaluacja

przeprowadzana jest przez Jednostkę Certyfikującą w systemie skonfigurowanym zgodnie z tymi parametrami technicznymi oraz o ile to możliwe z pozostałymi parametrami systemu (nie objętymi wytycznymi) ustawionymi w sposób przypadkowy.

## 4. Wymagania dotyczące zgodności w obszarze S

### 4.1. Opis certyfikatu

Certyfikat zgodności S wydawany jest dla obszaru bezpieczeństwa rozumianego zarówno jako bezpieczeństwo użycia (w tym bezpieczeństwo życia, zdrowia, aktywów i środowiska naturalnego) jak i poufność użycia (bezpieczeństwo informacji). Obejmuje on charakterystyki modelu SQuaRE „Safety in use” oraz „Security in use”. Certyfikat wydawany jest dla określonych w Deklaracji Zgodności obszarów zastosowania. Zakłada się, iż ze względu na specyfikę ewaluacji w zakresie Znak jakości S niezbędna jest bardzo ścisła współpraca pomiędzy Zgłaszającym a Jednostką Certyfikującą. Współpraca ta dotyczy przede wszystkim zagadnień związanych z zachowaniem poufności wyników ewaluacji oraz przekazaniem przez Zamawiającego do Jednostki Certyfikującej niezbędnej dokumentacji.

Bezpieczeństwo oprogramowania jako produktu jest pojęciem bardzo silnie związanym z pojęciem bezpieczeństwa infrastruktury i systemu w ramach którego oprogramowanie funkcjonuje. Stąd też oprócz deklaracji zgodności specyfikującej biznesowe konteksty użycia ewaluacji podlegają wytyczne dot. bezpieczeństwa systemu w ramach którego oprogramowanie jest uruchamiane.

### 4.2. Symbol certyfikatu

Nadanie certyfikatu wiąże się z przyznaniem prawa do stosowania dla konkretnego numeru wersji znaku towarowego S, który zaprezentowany jest na rysunku 3.



Rys. 3. - Znak potwierdzający zgodność w obszarze Bezpieczeństwa

Przy znaku podaje się poziom certyfikacji (patrz rozdział 4.3), dokładny numer wersji oraz informacje o miejscu w którym można zapoznać się z deklaracją zgodności specyfikującą biznesowe konteksty użycia, oraz wytyczne dot. bezpieczeństwa systemu w ramach którego oprogramowanie będzie uruchamiane.

### 4.3. Poziomy certyfikacji

Obszar certyfikacji na zgodność z wymogami bezpieczeństwa obejmuje w obecnej wersji Systemu Oceny Zgodności Oprogramowania jeden poziom. Dla tego poziomu opisano szczegółowe wymagania, jakie produkt musi spełniać. Przyznanie produktowi poziomu certyfikatu wiąże się z poświadczeniem przez Jednostkę Certyfikującą spełnienia wszystkich wymogów dla tego poziomu (w sytuacji kiedy wynik choćby jednego pomiaru nie spełnia wymagań minimalnych określony poziom certyfikacji nie może być przyznany). Pod

pojęciem wymogów rozumie się Listę profili bezpieczeństwa przypisaną do odpowiedniego obszaru. Lista ta grupuje Profile bezpieczeństwa będące uniwersalnym opisem najlepszych praktyk związanych z bezpieczeństwem w zakresie zdefiniowanym dla obszaru.

Lista obszarów dla Znak jakości S:

1. Bezpieczeństwo użycia (Safety in use)
  - a. Zagrożenia dla zdrowie i życia (Heath and life)
  - b. Zagrożenia dla aktywów (Assets)
  - c. Zagrożenia dla środowiska naturalnego (Life environment)
2. Poufność użycia (Security in use)
  - a. Poufność (Confidentiality)
  - b. Integralność (Integrity)
  - c. Dostępność (Availability)
  - d. Identyfikacja i autentykacja (Identification and authentication)
  - e. Rozliczalność (Accountability)
  - f. Autentyczność (Autenticity)
  - g. Niezaprzeczalność (Undeniability)
  - h. Niezawodność (Reliability)

#### 4.4. Wymagania szczegółowe

W niniejszym rozdziale opisano podstawowe wymogi dla wszystkich obszarów zastosowań. W przypadku określenia w deklaracji kontekstów użycia, należy uzupełnić zestaw mierzonych parametrów o parametry wynikające z danego kontekstu użycia. W przypadku braku określenia miar dla wskazanego kontekstu użycia Jednostka Certyfikująca wspólnie ze Zgłaszającym oraz Radą Jednostek Certyfikujących dokonuje analizy ryzyk związanych ze stosowaniem produktu dla tego kontekstu użycia publikując wymagania na stronach SASO zgodnie z procedurą opisaną w rozdziale 2.3.

##### 4.4.1. Poziom podstawowy

<b>Wymaganie</b>	<b>Wymagana cecha (miara)</b>	<b>Odniesienie do modelu</b>
Oprogramowanie zapewnia poufność informacji	Oprogramowanie uniemożliwia dostęp (celowy i przypadkowy) do zgromadzonych w nim informacji osobom/programom nieupoważnionym do uzyskania dostępu.	Security in use / Confidentiality
Oprogramowanie zapewnia spójność informacji	Oprogramowanie uniemożliwia modyfikację danych zgromadzonych w oprogramowaniu (w sposób celowy i przypadkowy) przez osobę/program nieupoważniony do wykonania modyfikacji. Oprogramowanie uniemożliwia zniszczenie informacji w nim zgromadzonych.	Security in use / Integrity

<b>Wymaganie</b>	<b>Wymagana cecha (miara)</b>	<b>Odniesienie do modelu</b>
Oprogramowanie zapewnia dostępność informacji	Oprogramowanie zapewnia możliwość uzyskania dostępu osobom/programom upoważnionym do otrzymania dostępu w czasie wynikającym z deklaracji zgodności.	Security in use / Availability
Oprogramowanie nie zagraża życiu i zdrowiu	W przypadku wpływu na bezpieczeństwo i zdrowie ludzi oprogramowanie posiada zabezpieczenia przed błędami mogącymi skutkować zagrożeniem życia i zdrowia.	Safety in use / Risks to the operator, risks to the public
Oprogramowanie nie zagraża mieniu	W przypadku wpływu na bezpieczeństwo mienia oprogramowanie posiada zabezpieczenia przed błędami mogącymi skutkować zagrożeniem dla mienia. Przez mienie rozumie się również wartości niematerialne takie jak reputacja firmy, jej własności niematerialne i prawne etc.	Safety in use / Commercial risks
Oprogramowanie nie zagraża środowisku	W przypadku wpływu na bezpieczeństwo środowiska oprogramowanie posiada zabezpieczenia przed błędami mogącymi skutkować zagrożeniem środowiska.	Safety in use / Risks to the environment
Oprogramowanie jest zgodne z wymaganiami formalnymi dla bezpieczeństwa	W przypadku oddziaływania na sferę bezpieczeństwa operatora, innych osób, mienia lub środowiska, lub w przypadku przechowywania informacji objętych ochroną (w tym tajemnicą przedsiębiorstwa użytkownika) oprogramowanie zapewnia poziom bezpieczeństwa zgodny z wymogami formalnymi dla tych obszarów.	Security in use, Safety in use / Compliance

Tab. 2. - *Wymagania szczegółowe dla certyfikacji S*

#### 4.5. Wymagania szczegółowe dotyczące ewaluacji

Proces ewaluacji jest ściśle związany z wymaganiami wynikającymi z deklarowanych kontekstów użycia oraz z wytycznymi związanymi z bezpieczeństwem systemu w ramach którego będzie uruchamiane oprogramowanie. Ewaluacja przeprowadzana jest przez Jednostkę Certyfikującą w systemie skonfigurowanym zgodnie z tymi wytycznymi oraz o ile to możliwe z pozostałymi parametrami systemu (nie objętymi wytycznymi) ustawionymi w sposób przypadkowy.



## 5. Wymagania dotyczące zgodności w obszarze §

### 5.1. Opis certyfikatu

Certyfikat zgodności § wydawany jest dla obszaru zgodności formalnej, a obejmuje wszelkie wymogi formalne dla oprogramowania wynikające z kontekstu użycia. Certyfikat stosowany jest dla określonych w Deklaracji Zgodności obszarów zastosowania. Wymagane jest aby w instrukcji użytkownika lub na stronie producenta widniała szczegółowa informacja na temat obszarów zastosowania produktu, dla której wydano certyfikat zgodności oraz wytycznych dot. sposobu użytkowania aplikacji oraz jej otoczeniu formalnym (np. informacje o tym jakie dodatkowe dokumenty powinny istnieć po stronie użytkownika, aby użycie oprogramowania było w pełni zgodne z wymogami formalnymi, jak choćby polityka przetwarzania danych osobowych).

### 5.2. Symbol certyfikatu

Nadanie certyfikatu wiąże się z przyznaniem prawa do stosowania dla konkretnego numeru wersji znaku towarowego §, który zaprezentowany jest na rysunku 4.



Rys. 4. - Znak potwierdzający zgodność w obszarze formalnym

Przy znaku podaje się poziom certyfikacji (patrz rozdział 5.3), dokładny numer wersji oraz informacje o miejscu w którym można zapoznać się z deklaracją zgodności specyfikująca biznesowe konteksty użycia, oraz datę dla której występuje zgodność z wymaganiami formalnymi (datę obowiązywania stanu prawnego) jak również wymogi formalne związane ze sposobem użytkowania oprogramowania.

### 5.3. Poziomy certyfikacji

Obszar certyfikacji obejmuje wszelkie charakterystyki jakościowe (w tym również objęte certyfikacją w ramach znaków E i S), ale pod kątem zgodności formalnej. Sposób certyfikacji rozpoczyna się od identyfikacji wymagań formalnych i wyspecyfikowaniu wynikających z nich charakterystyk i pod-charakterystyk jakościowych oraz konkretnych miar i ich oczekiwanych wartości. Przyznanie produktowi odpowiedniego poziomu certyfikatu wiąże się z poświadczeniem przez Jednostkę Certyfikującą spełnienia wszystkich wymogów dla danego poziomu (w sytuacji kiedy wynik choćby jednego pomiaru nie spełnia wymagań minimalnych określony poziom certyfikacji nie może być przyznany).

## 5.4. Wymagania szczegółowe

W niniejszym rozdziale opisano podstawowe wymogi dla wszystkich obszarów zastosowań. W przypadku określenia w deklaracji kontekstów użycia, należy uzupełnić zestaw mierzonych parametrów o parametry wynikające z danego kontekstu użycia. W przypadku braku określenia miar dla wskazanego kontekstu użycia Jednostka Certyfikująca wspólnie ze Zgłaszającym oraz Radą Jednostek Certyfikujących dokonuje analizy ryzyk związanych ze stosowaniem produktu dla tego kontekstu użycia publikując wymagania na stronach SASO zgodnie z procedurą opisaną w rozdziale 2.3.

### 5.4.1. Poziom podstawowy

<b>Wymaganie</b>	<b>Wymagana cecha (miara)</b>	<b>Odniesienie do modelu</b>
Oprogramowanie jest zgodne z wymaganiami formalnymi dla szybkości pracy i łatwości dostosowania, o ile takie występują	W przypadku oprogramowania użytkowanego przez określone grupy użytkowników (np. z ograniczeniami ruchowymi i percepcyjnymi) lub w określonych miejscach (np. miejsca o dużym natężeniu światła i dźwięku) oprogramowanie spełnia wymagania formalne dla takich sposobów użycia.	Usability in use, Adaptability in use / Compliance
Oprogramowanie jest zgodne z wymaganiami formalnymi dla bezpieczeństwa	W przypadku oddziaływania na sferę bezpieczeństwa operatora, innych osób, mienia lub środowiska, lub w przypadku przechowywania informacji objętych ochroną (w tym tajemnicą przedsiębiorstwa użytkownika) oprogramowanie zapewnia poziom bezpieczeństwa zgodny z wymogami formalnymi dla tych obszarów.	Security in use, Safety in use / Compliance
Oprogramowanie jest zgodne z przepisami dotyczącymi przetwarzania danych zgromadzonych w oprogramowaniu	Oprogramowanie przetwarza i utrzuła dane w sposób zgodny z przepisami, a w szczególności z ustawą o ochronie danych osobowych, ustawą o rachunkowości, ustawą prawo bankowe, ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne itd.	Context in use / Compliance
Oprogramowanie jest zgodne z wymaganiami dla biznesowego kontekstu użycia	Oprogramowanie spełnia wymagania formalne dla obszarów użycia wynikających z deklaracji zgodności.	Context in use / Compliance
Oprogramowanie jest wolne od wad prawnych	Oprogramowanie składa się wyłącznie z komponentów, których użycie jest zgodne z prawem.	

Tab. 3. - *Wymagania szczegółowe dla certyfikacji §*



### 5.5. Wymagania szczegółowe dotyczące ewaluacji

Użycie oprogramowania zgodnie z wymogami formalnymi wymaga tego, aby zarówno oprogramowanie, jak i sposób jego użytkowania były zgodne z wymaganiami. Z tego też powodu ewaluacji poddawane są wymogi wynikające z Deklaracji zgodności przygotowanej przez Zgłaszającego wraz z wytycznymi dot. sposobu użytkowania aplikacji przyjmując, że wszystkie rzeczy nie określone w wytycznych dot. sposobu użytkowania oprogramowania nie występują po stronie użytkownika.

## 6. Wzór deklaracji zgodności dla certyfikatu E

### DEKLARACJA ZGODNOŚCI Z WYMOGAMI ERGONOMII



*<Oznaczenie podmiotu składającego deklarację>*

Oświadczam, iż oprogramowanie o *<Nazwa oprogramowania>*, w wersji *<Nr wersji>* jest zgodnie z wymaganiami ergonomii zawartymi w Polskim Systemie Oceny Zgodności Oprogramowania.

Badania efektywności przeprowadzono w oparciu o infrastrukturę *<opis wszystkich elementów wpływających na efektywność i użyteczność oprogramowania>* w dniach *<data badania>* przez Jednostkę Certyfikującą *<nazwa Jednostki Certyfikującej>* działającą na podstawie umowy z Polskim Stowarzyszeniem na rzecz Atestacji i Standaryzacji Oprogramowania.

Oprogramowanie spełnia podstawowe wymagania zgodności *<oraz wymagania dla następujących obszarów użycia: ....>*.

Zalecenia producenta dla sposobu instalacji, konfiguracji i użytkowania mające na celu osiągnięcie deklarowanego poziomu efektywności opisane są *<link lub odniesienie do instrukcji użytkownika gdzie opisane są parametry jakie należy ustawić oraz zasady nadzoru i pielęgnacji pozwalające utrzymać poziom efektywności>*.

## 7. Wzór deklaracji zgodności dla certyfikatu S

### DEKLARACJA ZGODNOŚCI Z WYMOGAMI BEZPIECZEŃSTWA



*<Oznaczenie podmiotu składającego deklarację>*

Oświadczam, iż oprogramowanie o *<Nazwa oprogramowania>*, w wersji *<Nr wersji>* jest zgodnie z wymaganiami bezpieczeństwa zawartymi w Polskim Systemie Oceny Zgodności Oprogramowania.

Badania bezpieczeństwa przeprowadzono w oparciu o infrastrukturę zawierającą następujące zabezpieczenia *<opis wszystkich elementów zabezpieczających wpływających na bezpieczeństwo oprogramowania>* w dniach *<data badania>* przez Jednostkę Certyfikującą *<nazwa Jednostki Certyfikującej>* działającą na podstawie umowy z Polskim Stowarzyszeniem na rzecz Atestacji i Standaryzacji Oprogramowania.

Oprogramowanie spełnia podstawowe wymagania zgodności *<oraz wymagania dla następujących obszarów użycia: ....>*.

Zalecenia producenta dla sposobu instalacji, konfiguracji i użytkowania mające na celu osiągnięcie deklarowanego poziomu bezpieczeństwa opisane są *<link lub odniesienie do instrukcji użytkownika gdzie opisane są parametry jakie należy ustawić oraz zasady nadzoru i pielęgnacji pozwalające utrzymać poziom bezpieczeństwa>*.

## 8. Wzór deklaracji zgodności dla certyfikatu §

### DEKLARACJA ZGODNOŚCI Z WYMOGAMI FORMALNYMI



*<Oznaczenie podmiotu składającego deklarację>*

Oświadczam, iż oprogramowanie o *<Nazwa oprogramowania>*, w wersji *<Nr wersji>* jest zgodnie z wymaganiami formalnymi zawartymi w Polskim Systemie Oceny Zgodności Oprogramowania.

Badania zgodności przeprowadzono w oparciu o następujące akty normatywne (wg stanu na dzień *<data>*) *<opis aktów: ustaw, norm, rozporządzeń, wytycznych jakie zidentyfikowano i wzięto pod uwagę w trakcie badania>* w dniach *<data badania>* przez Jednostkę Certyfikującą *<nazwa Jednostki Certyfikującej>* działającą na podstawie umowy z Polskim Stowarzyszeniem na rzecz Atestacji i Standaryzacji Oprogramowania.

Oprogramowanie spełnia podstawowe wymagania zgodności *<oraz wymagania dla następujących obszarów użycia: ....>*.

Zalecenia producenta dla sposobu instalacji, konfiguracji i użytkowania mające na celu osiągnięcie deklarowanego poziomu zgodności formalnej opisane są *<link lub odniesienie do instrukcji użytkownika gdzie opisane są parametry jakie należy ustawić, oraz uregulowania w firmie użytkującej oprogramowanie, aby użytkowanie było zgodne z wymogami>*.



## 9. Odnosniki

---

<sup>1</sup> McCall J., Richards P., Walters G., Factors In software quality, Griffiths Air Force Base, NY, Rome Air Development Center Air Force Systems Command, 1977

<sup>2</sup> Boehm B., Brown J., Lipow M., MacCleod G, Characteristics of software quality, NY, American Elsevier, 1978

<sup>3</sup> Suryn W., Abran A., ISO/IEC SQuaRE. The second generation of standards for software product quality, IASTED2003

<sup>4</sup> W chwili publikacji dokumentu w fazie głosowania znajduje się wersja 55 dokumentu zawierająca inny podział na charakterystyki główne

<sup>5</sup> Źródło: <http://pl.wikipedia.org>

<http://www.measuringusability.com/papers/p482-sauro.pdf>