

Spis treści

Wprowadzenie	14
SEKCJA 1 – POSTANOWIENIA OGÓLNE	16
1 Zakres normy	16
2 Powołania normatywne	17
2.1 Identyczne rekomendacje Normy Międzynarodowe	17
2.2 Pary rekomendacji Normy Międzynarodowe równoważne w zawartości technicznej	18
3 Definicje	18
3.1 Definicje architektury bezpieczeństwa Modelu Odniesienia ISO	18
3.2 Definicje modelu Katalogu	19
3.3 Definicje	19
4 Skróty	22
5 Konwencje	22
6 Przegląd schematów	23
6.1 Podpisy cyfrowe	24
SEKCJA 2 – SCHEMAT CERTYFIKATU KLUCZA PUBLICZNEGO	26
7 Klucze publiczne i certyfikaty kluczy publicznych	27
7.1 Generacja pary kluczy	31
7.2 Tworzenie certyfikatu klucza publicznego	32
7.3 Ważność certyfikatu	32
8 Certyfikat klucza publicznego i rozszerzenia list CRL	35
8.1 Stosowanie polityki	36
8.1.1 Polityka certyfikacji	36
8.1.2 Certyfikacja poprzeczna	36
8.1.3 Odzworowanie polityki	38
8.1.4 Przetwarzanie ścieżki certyfikacji	38
8.1.5 Certyfikaty wydane przez samych siebie	38
8.2 Rozszerzenia z informacją o kluczu i polityce	39
8.2.1 Wymagania	39
8.2.2 Pola rozszerzeń w certyfikacie klucza publicznego i w liście CRL	40
8.2.2.1 Rozszerzenie identyfikator klucza organu	40
8.2.2.2 Rozszerzenie identyfikator klucza podmiotu	41
8.2.2.3 Rozszerzenie stosowanie klucza	41
8.2.2.4 Rozszerzenie rozszerzone stosowanie kluczy	42
8.2.2.5 Rozszerzenie okres stosowania klucza prywatnego	42
8.2.2.6 Rozszerzenie polityki certyfikacji	43
8.2.2.7 Rozszerzenie odzworowania polityki	44
8.3 Rozszerzenia informacja o podmiocie i wydawcy	45
8.3.1 Wymagania	45
8.3.2 Pola rozszerzeń certyfikatu i listy CRL	45
8.3.2.1 Rozszerzenie alternatywna nazwa podmiotu	45
8.3.2.2 Rozszerzenie alternatywna nazwa wydawcy	47
8.3.2.3 Rozszerzenie atrybuty katalogu podmiotów	47
8.4 Rozszerzenia ograniczenia ścieżki certyfikacji	47
8.4.1 Wymagania	47
8.4.2 Pola rozszerzeń certyfikatu	48
8.4.2.1 Rozszerzenie podstawowe ograniczenia	48
8.4.2.2 Rozszerzenie ograniczenia na nazwy	49
8.4.2.3 Rozszerzenie ograniczenia na politykę	50
8.4.2.4 Rozszerzenie powstrzymaj dowolną politykę	51
8.5 Podstawowe rozszerzenia list CRL	51
8.5.1 Wymagania	51

8.5.2	Pola rozszerzeń list CRL i wpisów CRL	52
8.5.2.1	Rozszerzenie numer listy CRL	52
8.5.2.2	Rozszerzenie kod przyczyny	53
8.5.2.3	Rozszerzenie kod instrukcji zatrzymania	54
8.5.2.4	Rozszerzenie data nieważności	54
8.5.2.5	Rozszerzenie zakres listy CRL	54
8.5.2.6	Rozszerzenie odsyłacz statusowy	57
8.5.2.7	Rozszerzenie identyfikator strumienia list CRL	58
8.5.2.8	Rozszerzenie uporządkowana lista	59
8.5.2.9	Rozszerzenie delta informacja	59
8.6	Punkty dystrybucji list CRL i rozszerzenia delta-list CRL	59
8.6.1	Wymagania	59
8.6.2	Pola rozszerzeń Punkt dystrybucji list CRL i delta-list CRL	60
8.6.2.1	Rozszerzenie punkty dystrybucji list CRL	61
8.6.2.2	Rozszerzenie wydający punkt dystrybucji	62
8.6.2.3	Rozszerzenie wydawca certyfikatu	63
8.6.2.4	Rozszerzenie wskaźnik delta listy CRL	63
8.6.2.5	Rozszerzenie aktualizacja bazy	64
8.6.2.6	Rozszerzenie najnowsza lista CRL	64
9	Relacja delta listy CRL z bazą	64
10	Procedura przetwarzania ścieżki certyfikacji	66
10.1	Dane wejściowe przetwarzania ścieżki	66
10.2	Dane wyjściowe przetwarzania ścieżki	67
10.3	Zmienne przetwarzania ścieżki	67
10.4	Krok inicjalizacji	67
10.5	Przetwarzanie certyfikatu	68
10.5.1	Podstawowe badania certyfikatu	68
10.5.2	Przetwarzanie pośrednich certyfikatów	68
10.5.3	Przetwarzanie jawnego wskaźnika polityki	69
10.5.4	Przetwarzanie końcowe	70
11	Schemat katalogu PKI	70
11.1	Klasy obiektów katalogu PKI i postaci nazw	70
11.1.1	Klasa obiektów użytkownik PKI	70
11.1.2	Klasa obiektów organ CA PKI	70
11.1.3	Klasa obiektów punkty dystrybucji list CRL i postać nazwy	71
11.1.4	Klasa obiektów delta listy CRL	71
11.1.5	Klasa obiektów polityka certyfikacji i CPS	71
11.1.6	Klasa obiektów ścieżka certyfikacji PKI	71
11.2	Atrybuty katalogu PKI	71
11.2.1	Atrybut certyfikat użytkownika	72
11.2.2	Atrybut certyfikat organu CA	72
11.2.3	Atrybut para certyfikatów poprzecznych	72
11.2.4	Atrybut lista unieważnionych certyfikatów	72
11.2.5	Atrybut lista unieważnionych organów	73
11.2.6	Atrybut delta listy unieważnień	73
11.2.7	Atrybut zapewniane algorytmy	73
11.2.8	Atrybut oświadczenie o praktyce certyfikacji	73
11.2.9	Atrybut polityka certyfikacji	74
11.2.10	Atrybut ścieżka PKI	74
11.3	Reguły zgodności katalogu PKI	74
11.3.1	Dokładna zgodność certyfikatów	74
11.3.2	Zgodność certyfikatów	75
11.3.3	Dokładna zgodność par certyfikatów	76
11.3.4	Zgodność par certyfikatów	76
11.3.5	Dokładna zgodność list certyfikatów	77
11.3.6	Zgodność list certyfikatów	77
11.3.7	Zgodność identyfikatorów algorytmu	78
11.3.8	Zgodność polityki	78
11.3.9	Zgodność ścieżki PKI	78

SEKCJA 3 – SCHEMAT CERTYFIKATU ATRYBUTYWNEGO	78
12 Certyfikaty atrybutywne.....	79
12.1 Struktura certyfikatu atrybutywnego	79
12.2 Ścieżki certyfikatów atrybutywnych	82
13 Powiązania – Organ Atrybutywny, SOA i Organ Certyfikacji	82
13.1 Uprawnienie w certyfikatach atrybutywnych	83
13.2 Uprawnienie w certyfikatach kluczy publicznych	83
14 Modele PMI	84
14.1 Model ogólny	84
14.1.1 PMI w kontekście kontroli dostępu	85
14.1.2 PMI w kontekście niezaprzeczalności	85
14.2 Model kontroli	86
14.3 Model delegacji	86
14.4 Modele ról	87
14.4.1 Atrybut roli	88
15 Rozszerzenia certyfikatów do zarządzania uprawnieniami.....	88
15.1 Rozszerzenia podstawowego zarządzania uprawnieniami	89
15.1.1 Wymagania	89
15.1.2 Pola rozszerzeń podstawowego zarządzania uprawnieniami	89
15.1.2.1 Rozszerzenie specyfikacja czasu	89
15.1.2.2 Rozszerzenie informacja podająca odbiorców	90
15.1.2.3 Rozszerzenie komunikat dla użytkownika	91
15.1.2.4 Akceptowalna polityka uprawnień	91
15.2 Rozszerzenia unieważnianie uprawnień.....	92
15.2.1 Wymagania	92
15.2.2 Pola rozszerzeń unieważnianie uprawnień	92
15.2.2.1 Rozszerzenie punkty dystrybucji list CRL.....	92
15.2.2.2 Rozszerzenie bez informacji o unieważnieniach	92
15.3 Rozszerzenia Źródła Uprawnień.....	92
15.3.1 Wymagania	92
15.3.2 Pola rozszerzeń SOA	93
15.3.2.1 Rozszerzenie identyfikator SOA	93
15.3.2.2 Rozszerzenie deskryptor atrybutu	93
15.4 Rozszerzenia ról	94
15.4.1 Wymagania	94
15.4.2 Pola rozszerzeń ról.....	95
15.4.2.1 Rozszerzenie identyfikator certyfikatu specyfikacji roli.....	95
15.5 Rozszerzenia delegacji.....	96
15.5.1 Wymagania	96
15.5.2 Pola rozszerzeń delegacji	96
15.5.2.1 Rozszerzenie podstawowe ograniczenia na atrybuty.....	96
15.5.2.2 Rozszerzenie delegowane ograniczenia na nazwy	98
15.5.2.3 Rozszerzenie akceptowalne polityki certyfikacji	98
15.5.2.4 Rozszerzenie identyfikator atrybutu organu	99
16 Procedura przetwarzania ścieżki uprawnień.....	100
16.1 Procedura przetwarzania podstawowego	100
16.2 Procedura przetwarzania roli	101
16.3 Procedura przetwarzania delegacji.....	101
16.3.1 Weryfikuj integralność reguły dominacji	102
16.3.2 Ustal ważną ścieżkę delegacji.....	102
16.3.3 Weryfikuj delegację uprawnień.....	102
16.3.4 Ustalenie przeszedł, nie przeszedł.....	103
17 Schemat katalogu PMI	103
17.1 Klasy obiektów katalogu PMI	103
17.1.1 Klasa obiektów użytkownik PMI	103
17.1.2 Klasa obiektów organ AA PMI	103
17.1.3 Klasa obiektów organ SOA PMI	103
17.1.4 Klasa obiektów punkt dystrybucji list CRL certyfikatów atrybutywnych.....	104

17.1.5	Klasa obiektów ścieżka delegacji PMI	104
17.1.6	Klasa obiektów polityka uprawnień	104
17.2	Atrybuty Katalogu PMI.....	104
17.2.1	Atrybut certyfikat atrybutywny	104
17.2.2	Atrybut certyfikat organu AA	104
17.2.3	Atrybut certyfikat deskryptora atrybutów	105
17.2.4	Atrybut lista unieważnionych certyfikatów atrybutywnych	105
17.2.5	Atrybut lista unieważnionych certyfikatów organów AA	105
17.2.6	Atrybut ścieżka delegacji.....	105
17.2.7	Atrybut polityka uprawnień	105
17.3	Ogólne reguły zgodności katalogu PMI	106
17.3.1	Dokładna zgodność certyfikatów atrybutywnych	106
17.3.2	Zgodność certyfikatów atrybutywnych	106
17.3.3	Zgodność posiadacza i wydawcy	107
17.3.4	Zgodność ścieżek delegacji	107
SEKCJA 4 – WYKORZYSTANIE SCHEMATU CERTYFIKATU KLUCZA PUBLICZNEGO I CERTYFIKATU		
ATRYBUTYWNEGO W KATALOGU.....		107
18	Uwierzytelnienie w Katalogu.....	107
18.1	Procedura zwykłe uwierzytelnienie.....	108
18.1.1	Generowanie chronionej informacji identyfikacyjnej	109
18.1.2	Procedura dla chronionego zwykłego uwierzytelnienia.....	109
18.1.3	Typ atrybutu Hasło Użytkownika	110
18.2	Mocne uwierzytelnienie	110
18.2.1	Otrzymywanie certyfikatów kluczy publicznych z katalogu	111
18.2.1.1	Przykład.....	112
18.2.2	Procedury mocnego uwierzytelnienia	114
18.2.2.1	Uwierzytelnienie jednokierunkowe	115
18.2.2.2	Uwierzytelnienie dwukierunkowe	116
18.2.2.3	Uwierzytelnienie trzykierunkowe	116
19	Kontrola dostępu.....	117
20	Ochrona operacji Katalogu	118
Załącznik A – Schematy certyfikatów kluczy publicznych i certyfikatów atrybutywnych.....		119
Załącznik B – Reguły generowania i przetwarzania list CRL.....		140
B.1	Wstęp	140
B.1.1	Typy list CRL	140
B.1.2	Przetwarzanie list CRL	141
B.2	Określenie Parametrów dla list CRL.....	142
B.3	Określenie potrzebnych list CRL	142
B.3.1	Podmiot zwykły z krytycznymi punktami CRL	143
B.3.2	Podmiot zwykły bez krytycznych punktów CRL DP	143
B.3.3	Organ CA z krytycznymi punktami CRL DP	143
B.3.4	Organ CA bez krytycznych punktów CRL DP	144
B.4	Otrzymaj listy CRL.....	144
B.5	Przetwórz listy CRL	144
B.5.1	Walidacja zakresu bazowej listy CRL	144
B.5.1.1	Kompletna lista CRL.....	145
B.5.1.2	Kompletna lista EPRL	145
B.5.1.3	Kompletna lista CARL	146
B.5.1.4	Lista CRL/EPRL/CARL z Punktu Dystrybucji	146
B.5.2	Walidacja zakresu delta listy CRL.....	147
B.5.3	Walidacja i sprawdzenie aktualności bazowej listy CRL	147
B.5.4	Walidacja i sprawdzenie delta listy CRL	148
Załącznik C – Przykłady wydawania delta list CRL		149
C.1	Wstęp	149
Załącznik D – Polityka uprawnień i przykłady definicji atrybutów		151

D.1	Wstęp.....	151
D.2	Przykładowe składnie	151
D.2.1	Pierwszy przykład.....	151
D.2.2	Drugi przykład	153
D.3	Przykład atrybutu uprawnień	155
Załącznik E – Wstęp do szyfrowania kluczem publicznym		156
Załącznik F – Definicja odniesienia identyfikatorów obiektów algorytm.....		158
Załącznik G – Przykłady stosowania ograniczeń na ścieżki certyfikacji		159
G.1	Przykład 1: Stosowanie podstawowych ograniczeń	159
G.2	Przykład 2: Stosowanie ograniczeń na nazwy.....	159
G.3	Przykład 3: Stosowanie odwzorowania polityki i ograniczeń na politykę.....	160
Załącznik H – Alfabetyczna lista definicji elementów informacji.....		161
Załącznik I – Zmiany i poprawki		164