

EN 419212-3:2017

Spis treści

Przedmowa do Normy Europejskiej	5
Wprowadzenie	6
1 Zakres normy	7
2 Powołania normatywne	7
3 Uwierzytelnianie urządzeń	7
3.1 Postanowienia ogólne	7
3.2 Wprowadzenie do uwierzytelniania asymetrycznego	8
3.3 Urzędy certyfikacji i certyfikaty	9
3.3.1 Łańcuchy certyfikatów	9
3.3.2 Stosowanie certyfikatów zakładkowych	9
3.4 Środowiska uwierzytelniania	10
3.4.1 SCA w środowisku zaufanym	10
3.4.2 SCA w środowisku niezaufanym	10
3.4.3 Określenie środowiska	11
3.4.4 Mechanizm wyświetlanego komunikatu	11
3.4.5 Dodatkowe środowiska uwierzytelniania	11
3.5 Mechanizmy transportu kluczy i uzgadniania kluczy	11
3.6 Uwierzytelnianie urządzeń z ochroną prywatności	12
3.6.1 Postanowienia ogólne	12
3.6.2 Kroki uwierzytelniania	12
3.7 Protokół modularny EAC (mEAC) z ograniczeniem prywatności bez możliwości śledzenia	29
3.7.1 Postanowienia ogólne	29
3.7.2 Przykład przypadku możliwości śledzenia	30
3.7.3 Notacja	30
3.7.4 Kroki uwierzytelniania	31
3.7.5 Mechanizm braku możliwości łączenia z indywidualnymi kluczami prywatnymi	43
3.8 Symetryczny schemat uwierzytelniania	50
3.8.1 Postanowienia ogólne	50
3.8.2 Kroki uwierzytelniania	51
3.8.3 Tworzenie kluczy sesyjnych	54
3.9 Protokół transportu kluczy oparty na RSA	55
3.9.1 Postanowienia ogólne	55
3.9.2 Kroki uwierzytelniania	56
3.9.3 Tworzenie kluczy sesyjnych	64
3.10 Obliczanie kluczy sesyjnych z ziarna klucza $K_{\text{IFD/ICC}}$	65
3.10.1 Postanowienia ogólne	65
3.10.2 Generowanie materiału kluczowego	65
3.10.3 Podział materiału kluczowego	66
3.10.4 Określenie specyficznej dla algorytmu metody derywacji kluczy	66
3.10.5 Derywacja kluczy z haseł	68
3.11 Inicjacja licznika wysyłanego ciągu poleceń i odpowiedzi SSC	70
3.12 Faza po uwierzytelnieniu	70
3.13 Zakończenie bezpiecznej sesji	70
3.13.1 Postanowienia ogólne	70
3.13.2 Przykład zakończenia bezpiecznej sesji	70
3.13.3 Zasady zakończenia bezpiecznej sesji	71
3.14 Odczyt wyświetlanego komunikatu	71
3.15 Aktualizacja wyświetlanego komunikatu	73
4 Struktury danych	74
4.1 Postanowienia ogólne	74
4.2 CRT	74

4.2.1	Postanowienia ogólne	74
4.2.2	CRT AT dla wyboru wewnętrznych prywatnych kluczy uwierzytelniających	74
4.2.3	CRT AT dla wyboru wewnętrznych kluczy uwierzytelniających	75
4.2.4	CRT dla wyboru PuK.CA _{IFD} .CS_AUT	75
4.2.5	CRT dla wyboru PuK.IFD. AUT	76
4.2.6	CRT AT dla wyboru parametrów klucza publicznego DH / ECDH	76
4.2.7	Parametry klucza DH dla GENERAL AUTHENTICATE wykorzystywane przez protokół z ochroną prywatności	77
4.2.8	CRT AT dla wyboru prywatnego klucza uwierzytelniającego ICC	77
4.2.9	CRT dla wyboru PuK.IFD. AUT	77
4.2.10	CRT dla wyboru PrK.ICC.KA	78
4.3	Protokół uwierzytelniania urządzeń z transportem kluczy	78
4.3.1	EXTERNAL AUTHENTICATE	78
4.3.2	INTERNAL AUTHENTICATE	79
4.4	Protokół uwierzytelniania urządzeń z ochroną prywatności	79
4.4.1	EXTERNAL AUTHENTICATE (przypadek DH)	79
4.4.2	EXTERNAL AUTHENTICATE (przypadek ECDH)	80
4.4.3	INTERNAL AUTHENTICATE (przypadek DH)	81
4.4.4	INTERNAL AUTHENTICATE (przypadek ECDH)	81
5	Certyfikaty CV i zarządzanie kluczami	82
5.1	Postanowienia ogólne	82
5.2	Poziom zaufania w certyfikacie	82
5.3	Zarządzanie kluczami	82
5.4	Rodzaje certyfikatów	83
5.4.1	Certyfikaty weryfikowalne przez kartę	83
5.4.2	Certyfikaty podpisu	84
5.4.3	Certyfikaty do uwierzytelniania	84
5.5	Stosowanie klucza publicznego wyodrębnionego z certyfikatu CV	84
5.6	Ważność klucza wyodrębnionego z certyfikatu CV	85
5.7	Struktura CVC	85
5.7.1	Postanowienia ogólne	85
5.7.2	Certyfikaty niesamoopisowe	86
5.7.3	Certyfikaty samoopisowe	86
5.8	Treść certyfikatu	86
5.8.1	Postanowienia ogólne	86
	Identyfikator profilu certyfikatu (CPI)	87
5.8.2	DO referencji urzędu certyfikacji (CAR)	88
5.8.3	DO referencji posiadacza certyfikatu (CHR)	89
5.8.4	CHA-Obiekt danych autoryzacji posiadacza certyfikatu (CHA-DO)	90
5.8.5	Określenie identyfikatora roli	92
5.8.6	Uwierzytelnianie użytkownika i dostawcy usługi	93
5.8.7	CHAT-Szablon autoryzacji posiadacza certyfikatu (CHAT)	94
5.8.8	OID – Identyfikator obiektu	94
5.8.9	CEDT – Szablon daty początku ważności certyfikatu	94
5.8.10	CXDT – Szablon daty wygaśnięcia certyfikatu	94
5.9	Podpis certyfikatu	95
5.9.1	Postanowienia ogólne	95
5.9.2	Certyfikaty niesamoopisowe	95
5.9.3	Certyfikaty samoopisowe	96
5.10	Kodowanie treści certyfikatu	96
5.10.1	Certyfikaty niesamoopisowe	96
5.10.2	Certyfikaty samoopisowe	97
5.10.3	Certyfikaty samoopisowe dla kryptografii krzywych eliptycznych	97
5.11	Kroki weryfikacji CVC	101
5.11.1	Postanowienia ogólne	101
5.11.2	Pierwsza runda: weryfikacja CVC z PuK głównego CA	102
5.11.3	Kolejne rundy	102
5.12	Polecenia do obsługi CVC	103
5.13	C_CV.IFD.AUT (niesamoopisowy)	103

EN 419212-3:2017

5.14 C_CV.CA.CS-AUT (niesamoopisowy) 104

5.15 C.ICC.AUT 106

5.16 Samoopisowy certyfikat CV (Przykład) 106

5.16.1 Postanowienia ogólne 106

5.16.2 Klucz publiczny 107

5.16.3 Szablon autoryzacji posiadacza certyfikatu 107

5.16.4 Rozszerzenie certyfikatu 107

5.16.5 Podpis ECDSA 108

Załącznik A (informacyjny) Właściwości protokołu uwierzytelniania urządzeń 109

Bibliografia 111