

2018

Řízení energetických soustav a přidružená výměna informací -
Bezpečnost dat a komunikací -
Část 9: Řízení klíčů kybernetické bezpečnosti
pro zařízení energetické soustavy

ČSN
EN 62351-9
33 5011

idt IEC 62351-9:2017

Power system management and associated information exchange - Data and communication security -

Part 9: Cyber security key management for power system equipment

Gestion des systemes de puissance et échanges d'informations associés - Sécurité des communications et des données -

Partie 9: Gestion de clé e cybersécurité des équipements de systeme de puissance

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation -

Teil 9: Cyber security Schlüssel-Management für Strom versorgungsanlagen

Tato norma je českou verzí evropské normy EN 62351-9:2017. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN 62351-9:2017. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

IEC TS 62351-2 nezavedena

ISO/IEC 9594-8:2017 (idt Doporučení ITU-T X.509:2016) dosud nezavedena

ISO/IEC 9834-1/:2012 (idt Doporučení ITU-T X.660:2011) dosud nezavedena

RFC 5246 nezaveden

RFC 5272 nezaveden

RFC 5934 nezaveden

RFC 6407 nezaveden

RFC 6960 nezaveden

RFC 7030 nezaveden

SCEP IETF Draft nezavedena

Informativní údaje z IEC 62351-9:2017

Mezinárodní normu IEC 62351-9 vypracovala technická komise IEC/TC 57 *Řízení elektrizačních soustav a výměna přidružených informací*.

Text této normy se zakládá na těchto dokumentech:

FDIS	Zpráva o hlasování
57/1838/FDIS	57/1853/RVD

Úplnou informaci o hlasování při schvalování této normy lze najít ve zprávě o hlasování ve výše uvedené tabulce.

Tato publikace byla vypracována v souladu se směrnicemi ISO/IEC, část 2.

Seznam všech částí souboru IEC 62351 se společným názvem *Řízení elektrizační soustavy a přidružená výměna informací - Bezpečnost dat a komunikací* je možno nalézt na webových stránkách IEC.

V této normě se používají následující typy písma:

- pojmy ASN.1 jsou uváděny tučně v písmu Courier New;
- pokud jsou odkazovány v normálním textu typy a hodnoty ASN.1, jsou odlišné od normálního textu tím, že jsou uvedeny tučně v písmu Courier.

Komise rozhodla, že obsah této publikace zůstane nezměněn až do data příští prověrky (stability date) uvedeného na webových stránkách IEC (<http://webstore.iec.ch>) v údajích o této publikaci. K tomuto datu bude publikace buď

- znovu potvrzena;
- zrušena;
- nahrazena revidovaným vydáním, nebo
- změněna.

UPOZORNĚNÍ - Publikace obsahuje barevný tisk, který je považován za potřebný k porozumění jejímu obsahu. Uživatelé by proto měli pro tisk tohoto dokumentu použít barevnou tiskárnu.

Vypracování normy

Zpracovatel: EGC - EnerGoConsult ČB, s. r. o., IČO 25166972, Petr Pražák

Technická normalizační komise: TNK 97 Elektroenergetika

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Milan Dian

ICS 33.200

Řízení energetických soustav a přidružená výměna informací -
Bezpečnost dat a komunikací -
Část 9: Řízení klíčů kybernetické bezpečnosti pro zařízení energetické soustavy
(IEC 62351-9:2017)

Power systems management and associated information exchange -
Data and communications security -
Part 9: Cyber security key management for power system equipment
(IEC 62351-9:2017)

Gestion des systemes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 9: Gestion de clé de cybersécurité des équipement de systeme de puissance (IEC 62351-9:2017)	Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 9: Cyber security Schlüssel-Management für Stromversorgungsanlagen (IEC 62351-9:2017)
--	--

Tato evropská norma byla schválena CENELEC dne 2017-06-22. Členové CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC nebo u kteréhokoliv člena CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Členy CENELEC jsou národní elektrotechnické komitety Belgie, Bulharska, Bývalé jugoslávské republiky Makedonie, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irsko, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polsko, Portugalsko, Rakousko, Rumunsko, Řecko, Slovensko, Slovinsko, Spojeného království, Srbsko, Španělsko, Švédsko, Švýcarsko a Turecko.



Evropský výbor pro normalizaci v elektrotechnice
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
Řídicí centrum CEN-CENELEC: Avenue Marnix 17, B-1000 Brusel

© 2017 CENELEC Veškerá práva pro využití v jakékoli formě a jakýmikoli prostředky jsou celosvětově vyhrazena členům CENELEC.

Ref. č. EN

62351-9:2017 E

Evropská předmluva

Text dokumentu 57/1838/FDIS, budoucího prvního vydání IEC 62351-9, vypracovala technická komise IEC/TC 57 *Řízení elektrizační soustavy a přidružená výměna informací*, byl předložen k paralelnímu hlasování IEC-CENELEC a byl schválen CENELEC jako EN 62351-9:2017.

Jsou stanovena tato data:

- nejzazší datum zavedení dokumentu na národní úrovni
vydáním identické národní normy nebo vydáním
oznámení o schválení k přímému používání
jako normy národní (dop) 2018-03-22
- nejzazší datum zrušení národních norem,
které jsou s dokumentem v rozporu (dow) 2020-06-22

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CENELEC nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Tento dokument byl vypracován na základě mandátu uděleném CENELEC Evropskou Komisí a Evropským sdružením volného obchodu.

Oznámení o schválení

Text mezinárodní normy IEC 62351-9:2017 byl schválen CENELEC jako evropská norma bez jakýchkoliv modifikací.

1..... Rozsah platnosti.....	
.....	9
2..... Citované dokumenty.....	
.....	9
3..... Termíny a definice.....	
.....	9
4..... Zkratky.....	
.....	14
5..... Šifrovací aplikace pro implementace v napájecí soustavě.....	15
5.1..... Šifrování, šifrovací klíče a bezpečnostní cíle.....	15
5.2..... Typy šifrování.....	16
5.3..... Použití šifrování.....	16
5.3.1... Cíle kybernetické bezpečnosti.....	16
5.3.2... Utajení.....	17
5.3.3... Integrita dat.....	17
5.3.4... Autentizace.....	17
5.3.5... Nezpochybnitelnost.....	17

5.3.6...

Důvěra.....
..... 17

6..... Koncepty a metody řízení klíčů v rámci operací v napájecí soustavě..... 18

6.1..... Bezpečnostní politika systému řízení klíčů..... 18

6.2..... Konstrukční zásady řízení klíčů pro operace v napájecí soustavě..... 18

6.3..... Použití zabezpečení na úrovni přenosové vrstvy (TLS)..... 18

6.4..... Použití šifrovacího klíče.....
..... 19

6.5..... Důvěra na základě infrastruktury s veřejným klíčem (PKI)..... 19

6.5.1... Registrační autorita (RA).....
... 19

6.5.2... Certifikační autorita (CA).....
... 19

6.5.3... Certifikáty veřejného klíče.....
. 19

6.5.4... Certifikáty atributů.....
..... 20

6.5.5... Rozšíření certifikátu veřejného klíče a certifikátu atributů..... 20

6.6..... Důvěra stanovená pomocí certifikátů podepsanými sami sebou, které nejsou PKI..... 20

6.7..... Autorizační a validační seznamy.....
21

6.7.1...
Obecně.....
..... 21

6.7.2... AVL v prostředí bez omezení	
.. 21	
6.7.3... AVL v prostředí s omezením	
..... 21	
6.7.4... Použití certifikátů veřejného klíče podepsaných sami sebou v AVL	22
6.8..... Důvěra definovaná pomocí předem sdílených klíčů	22
6.9..... Relační klíče	
..... 22	
6.10... Protokoly používané při ustanovení důvěry	22
6.10.1 Požadavek certifikace	
..... 22	
6.10.2 Protokol řízení pevných bodů důvěry (TAMP)	22
6.10.3 Protokol pro jednoduchý zápis certifikátu (SCEP)	23
6.10.4 Internetový protokol řízení certifikátu X.509 PKI (CMP)	23
6.10.5 Řízení certifikátu přes CMS (CMC)	23
6.10.6 Registrace přes zabezpečený přenos (EST)	23
6.10.7 Souhrnný pohled na různé protokoly	23
6.11... Skupinové klíče	
..... 24	

6.11.1 Účel skupinových klíčů.....	
.....	24
6.11.2 Skupinová oblast interpretace (GDOI).....	24
6.12.... Životní cyklus řízení klíče.....	
....	28
6.12.1 Řízení klíče v rámci životního cyklu entity.....	28
6.12.2 Životního cyklu šifrovacího klíče.....	30
6.13.... Procesy řízení certifikátů.....	
.....	31
6.13.1 Proces řízení certifikátu.....	
.....	31
6.13.2 Počáteční vytvoření certifikátu.....	
... 31	
6.13.3 Zapsání entity.....	
.....	31
6.13.4 Proces žádost o podepsání certifikátu (CSR).....	34
6.13.5 Seznamy odvolaných certifikátů (CRL).....	34
6.13.6 Stavový protokol online certifikace (OCSP).....	35
6.13.7 Protokol pro ověření certifikátu využívající server (SVCP).....	37
6.13.8 Krátkodobé certifikáty.....	
.....	38
6.13.9 Obnovení certifikátu.....	

.....	38
6.14.... Alternativní proces pro asymetrické klíče, které nejsou generované entitou.....	40
6.15.... Distribuce klíče v případě symetrických klíčů s různými časovými rámci.....	41
7..... Požadavky na řízení generálního klíče.....	41
7.1..... Požadavky na řízení asymetrického a symetrického klíče.....	41
7.2..... Požadovaný šifrovací materiál.....	41
7.3..... Požadavky na certifikáty veřejného klíče.....	41
7.4..... Ochrana šifrovacího klíče.....	42
7.5..... Využití stávající infrastruktury pro řízení klíčů.....	42
7.6..... Použití identifikátorů objektů.....	42
8..... Řízení asymetrických klíčů.....	42
8.1..... Generování a instalace certifikátu.....	42
8.1.1... Generování a instalace privátního a veřejného klíče.....	42
8.1.2... Obnovení privátního a veřejného klíče.....	42
8.1.3... Generování náhodného čísla.....	42
8.1.4... Certifikační politika.....	43

8.1.5... Registrace entity za účelem jejího zřízení.....	43
8.1.6... Konfigurace entity.....	43
8.1.7... Zápis entity.....	43
8.1.8... Aktualizace informací týkajících se pevného bodu důvěry.....	44
8.2..... Odvolání certifikátu veřejného klíče.....	45
8.3..... Platnost certifikátu.....	45
8.3.1... Platnost certifikátů.....	45
8.3.2... Odvolání certifikátu.....	46
8.3.3... Kontrola stavu odvolání certifikátu.....	46
8.3.4... Práce s autorizačními a validačními seznamy (AVL).....	46
8.4..... Vypršení platnosti a obnovení certifikátu.....	51
8.5..... Zabezpečená synchronizace času.....	51

9..... Řízení symetrických klíčů.....	
... 51	
9.1..... Řízení skupinových klíčů (GDOI).....	51
9.1.1... Požadavky GDOI.....	51
9.1.2... Internetová výměna klíče, verze 1 (IKEv1).....	51
9.1.3... Hlavní režim výměny typ 2 fáze 1 IKEv1.....	52
9.1.4... Informativní výměna typu 5 fáze 1 ISAKMP.....	56
9.1.5... Výměna GDOI GROUPKEY-PULL typ 32 fáze 2.....	57
9.1.6... Výměna stažení skupinového klíče GROUPKEY-PULL.....	64
10..... Návaznost na části IEC 62351 a ostatní dokumenty IEC.....	65
Příloha A (normativní) Prohlášení o souladu s implementací protokolu (PICS).....	66
Příloha B (informativní) Generování náhodného čísla.....	67
B.1..... Způsoby generování náhodného čísla.....	66
B.2..... Deterministické generátory náhodných čísel.....	66
B.3..... Nedeterministické generátory náhodných čísel.....	66
B.4..... Zdroje entropie.....	67
Příloha C (informativní) Schéma průběhu zápisu a obnovení certifikátu.....	69

C.1..... Zápis certifikátu.....	68
C.2..... Obnovení certifikátu.....	68
Příloha D (informativní) Příklady certifikačních profilů.....	71
Bibliografie.....	75
Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a jim odpovídající evropské publikace.....	77
Obrázek 1 - Vazba mezi certifikáty veřejného klíče a certifikáty atributů.....	20
Obrázek 2 - Distribuce řízení skupinových klíčů.....	24
Obrázek 3 - GDOI IKE Fáze 1 - Autentizace a zabezpečení komunikačního kanálu.....	25
Obrázek 4 - GDOI Pull Fáze 2..... . 25	
Obrázek 5 - Obnovení klíče spouštěné entitami.....	27
Obrázek 6 - Řízení klíče během životního cyklu produktu.....	28
Obrázek 7 - Zjednodušený životní cyklus certifikátu.....	29
Obrázek 8 - Životní cyklus šifrovacího klíče.....	30
Obrázek 9 - Příklad zápisu entity SCEP a procesu CSR.....	32
Obrázek 10 - Příklad zápisu EST entity a CSR procesu.....	33
Obrázek 11 - Zpracování CSR.....	34
Obrázek 12 - Seznam odvolaných	

certifikátů.....	35
Obrázek 13 - Přehled stavového protokolu online certifikátu.....	36
Obrázek 14 - Schéma zobrazující kombinaci procesů CRL a OCSP.....	36
Obrázek 15 - Toky volání u stavového protokolu online certifikátu (OCSP).....	37
Obrázek 16 - Přehled protokolu SVCP používajícího backend OCSP.....	37
Obrázek 17 - Obnovení certifikátu SCEP.....	39
Obrázek 18 - Obnovení/překlíčování certifikátu EST.....	40
Obrázek 19 - Generování ústředního klíče.....	41
Obrázek 20 - Hlavní režim výměny IKEv1 (RFC 2409) s digitálním podpisem RSA.....	53
Obrázek 21 - Hlavní režim výměny IKEv1 a zprávy spojené se zabezpečením.....	53
Obrázek 22 - Hlavní režim výměny IKEv1: Zprávy týkající se výměny klíče.....	54

Obrázek 23 - Hlavní režim výměny IKEv1: Zprávy autentizace ID.....	55
Obrázek 24 - Výpočet HASH_I IKEv1.....	55
Obrázek 25 - Informativní výměna fáze 1.....	56
Obrázek 26 - GD004FI GROUPKEY-PULL definovaná v RFC 6407.....	57
Obrázek 27 - Výpočty hašování GROUPKEY- PULL.....	57
Obrázek 28 - Úvodní výměna Požadavku SA GROUPKEY- PULL.....	58
Obrázek 29 - Obsah Identifikace RFC 6407.....	58
Obrázek 30 - Identifikační data ID_OID.....	59
Obrázek 31 - ASN.1 BNF pro 61850_UDP_ADDR_GOOS/SV.....	60
Obrázek 32 - ASN.1 BNF IPADDRESS..... ... 61	61
Obrázek 33 - Příklad ASN.1 dat IecUpdAddrPayload s kódováním DER.....	61
Obrázek 34 - Obsah ASN.1 BNF 61850_UPD_TUNNEL.....	61
Obrázek 35 - Obsah ASN.1 BNF 61850_ETHERNET_GOOSE/SV.....	62
Obrázek 36 - Obsah TEK SA RFC 6407.....	62
Obrázek 37 - Obsah TEK SA IEC-61850.....	63
Obrázek 38 - Výměna stažení klíče GROUPKEY- PULL.....	64
Obrázek 39 - Vazby IEC 62351 Část 9 na ostatní části IEC	

62351.....	65
Obrázek C.1 - Zápis certifikátu.....	69
Obrázek C.2 - Konečný automat obnovení certifikátu.....	70
Tabulka 1 - Požadavky IKEv1 pro KDC.....	52
Tabulka 2 - ID Objektů IEC 61850: Povinné (m) a nepovinné (o).....	60
Tabulka D.1 - Příklady certifikátů veřejného klíče provozovatele.....	72
Tabulka D.2 - Příklady certifikátů OEM.....	73
Tabulka D.3 - Příklady certifikátů OCSP.....	74

1 Rozsah platnosti

Tato norma specifikuje řízení šifrovacích klíčů, konkrétně jakým způsobem se vytváří, distribuují, ruší a pracuje s certifikáty veřejných klíčů a šifrovacími klíči sloužícími k ochraně digitálních dat a komunikací. Rozsah platnosti zahrnuje i práci s asymetrickými klíči (například privátní klíče a certifikáty veřejných klíčů) i asymetrickými klíči pro skupiny (GDOI).

Tato norma předpokládá, že typ klíčů a šifrování, které se bude používat, již bylo zvoleno pomocí jiných norem, jelikož volba těchto šifrovacích algoritmů a klíčů se obvykle řídí vlastními bezpečnostními politikami společnosti a potřebou splňovat ostatní mezinárodní normy. Tento dokument tudíž specifikuje pouze metody řízení těchto zvolených infrastruktur klíčů a šifrování. Úkolem je definovat požadavky a technologie k dosažení interoperability.

Smyslem této normy je zaručit interoperabilitu mezi různými prodejci tím, že se stanoví nebo vymezí používané varianty řízení klíčů. Tento dokument předpokládá, že čtenář rozumí principům šifrování a PKI.

Konec náhledu - text dále pokračuje v placené verzi ČSN.