

Specifikace formátu QR jízdenka

Mobilní aplikace pro integrovaný dopravní systém Královéhradeckého a Pardubického kraje

Specifikace formátu QR jízdenka

Status dokumentu: veřejný

Verze: 1.0, ze dne 21. 8. 2024

Obsah

Obsah	1
Informace o dokumentu	2
Historie změn	2
Seznam příloh	2
Seznam použitých zkratk	2
Specifikace formátu QR jízdenka	3
Popis formátu	3
Základní atributy	3
Klíče atributů	3
Hodnoty atributů	3
Formáty hodnot atributů	3
Zajištění a ověření pravosti	5
Generování podpisu ETD SG	5
Ověření podpisu ETD SG	5
Ověření platnosti	5
Ukládání a sdílení	5
Příklad	6

Informace o dokumentu

Historie změn

Datum	Verze	Stav	Autor
21. 8. 2024	1.0	První verze dokumentu.	CHAPS

Seznam příloh

Označení	Popis

Seznam použitých zkratk

Zkratka	Význam zkratky
CHAPS	CHAPS spol. s r.o., poskytovatel
Offline	Indikuje stav absence připojení k internetu / síti
Online	Indikuje stav připojení k internetu / síti
QR	Quick Response, QR kód
ETD	Electronic Ticket Deskriptor, elektronický popis jízdenky
ECDSA	Elliptic Curve Digital Signature Algorithm, digitální podpis s využitím eliptických křivek
HTTP	Hypertext Transfer Protocol, protokol pro výměnu informací na Internetu
MIME	Multipurpose Internet Mail Extensions, protokol pro výměnu informací na Internetu

Specifikace formátu QR jízdenka

- Formát QR jízdenka je navržen jako otevřený formát s možností využití u dalších dopravců a koordinátorů.
- Specifikace vychází z úspěšně přijatého formátu QR platba (<https://qr-platba.cz>).
- Cílem je univerzálně použitelný snadno čitelný a volitelně rozšiřitelný textový popis elektronické jízdenky (dále také ETD, Electronic Ticket Descriptor)
- Ověření pravosti elektronické jízdenky je zajištěno elektronickým podpisem s využitím asymetrické kryptografie.
- Jako nosič elektronické jízdenky je použit QR kód, ale formát nevylučuje použití jiného 2D kódu, textové podoby nebo přenos formou NFC.

Popis formátu

Formát řetězce je navržen tak, aby byl kompaktní co se velikosti obsažených dat týče. Výhodou navrženého formátu je relativně dobrá lidská čitelnost a potenciální rozšiřitelnost o specifické atributy.

Řetězec může obsahovat libovolné znaky ze znakové sady ISO-8859-1 (znaková sada pro [binární QR kód](#)). Pro efektivní uložení do QR kódu doporučujeme sestavit řetězec tak, aby obsahoval pouze následující znaky:

- 0–9
- A–Z (pouze velká písmena)
- mezera
- \$, %, *, +, -, ., /, :

Při zachování znaků výhradně z uvedené množiny bude použit tzv. alfanumerický formát QR kódu. Množina znaků používaná v klíších a řídicích strukturách navrženého formátu je proto volena právě z této množiny tak, aby nebylo zabráněno dosažení maximální možné efektivity uložení platebních informací do QR kódů. Bude-li v hodnotě kteréhokoli pole použit znak z jiné množiny, než je uvedena výše, bude použit tzv. binární formát QR kódu.

Řetězec je vždy zahájen fixní hlavičkou ETD*. Následuje verze protokolu (jedno nebo dvě čísla oddělená tečkou) ukončená hvězdičkou, např. 1.0*. Následně řetězec obsahuje jednotlivé atributy platby ve formátu *klíč:hodnota**, tedy klíč je od hodnoty oddělen dvojtečkou, za hodnotou následuje hvězdička.

Délka řetězce ETD by měla být co nejkratší pro dosažení nízké komplexity vygenerovaného QR kódu. Celková délka řetězce ETD nesmí přesáhnout 4 296 znaků.

Základní atributy

Klíče atributů

- jsou vždy zapsány velkými znaky z množiny znaků [A-Z],
- seznam přípustných klíčů (základní sada atributů) je uveden v tabulce níže,
- formát může být rozšířen o proprietární klíče, které mají např. lokální význam pro konkrétního vydavatele. Takovéto klíče jsou uvozeny znaky X-.

Hodnoty atributů

- musí být v přípustném formátu pro dané pole – viz formáty hodnot atributů,
- nesmí začínat ani končit bílými znaky,
- nesmí obsahovat znak * (hvězdička)
- může obsahovat znak : (dvojtečka).
- může obsahovat speciální znaky kódované pomocí URL kódování. Díky tomuto mechanismu je možné kódovat libovolné znaky z UTF-8, hvězdičku je tedy možno do hodnoty zahrnout pomocí zápisu %2A.

Formáty hodnot atributů

- text
 - přípustné znaky [0-9A-Z \$%+-.:/]
- datum a čas

- zápis podle normy ISO 8601
- tj. ve formátu YYYY-MM-DD, YYYY-MM-DD'T'hh:mm:ss, YYYY-MM-DD'T'hh:mm:ss'Z'ZZZZ
- časová zóna nemusí být uvedena, pokud je jízdenka platná v jedné lokální časové zóně
- přípustné znaky [0-9TZ+-:]
- celé číslo
 - přípustné znaky [0-9]
- desetinné číslo
 - oddělovač desetinná tečka
 - přípustné znaky [0-9.]

Klíč	Formát	Hodnota	Příklad zápisu klíče a hodnoty
IN	text	Identifikace vydavatele. Typicky zkratka dopravního podniku či koordinátora	IN:DPP*
IS	text	Název nebo identifikátor výdejce	IS:6-1234*
IT	celé číslo	Časové razítko vygenerování ETD. Počet sekund od 1.1.1970 0:00:00 UTC	IT:1511543112*
TI	text	Jednoznačný identifikátor jízdenky	TI:1001235*
TT	text	Označení druhu jízdenky nebo tarifu	TT:DPT24*
TP	desetinné číslo, mezeru, text	Cena jízdenky, volitelně včetně měny (zkratka dle ISO) oddělené mezerou	TP:24.00 CZK*
FR	text	Výchozí stanice	FR:HLAVNI NADRAZI*
TO	text	Cílová stanice	TO:VYSEHRAD*
VS	datum a čas	Platnost od (včetně)	VS:2018-02-15T18:00:35*
VU	datum a čas	Platnost do (včetně)	VU:2018-02-16T18:00:35*
VL	text	Seznam spojů, ve kterých je jízdenka platná, oddělených čárkou	VL:IC160*
VC	text	Seznam tříd, ve kterých je jízdenka platná, oddělených čárkou	VC:2*
VZ	text	Seznam zón, ve kterých je jízdenka platná, oddělených čárkou	VZ:P,0,B*

HN	text	Jméno držitele	HN:JAN*
HS	text	Příjmení držitele	HS:NOVAK*
HI	text	Identifikátor držitele	HI:ID-8412220510*
RL	text	Seznam spojů, ve kterých má držitel rezervace, oddělených čárkou	RL:IC160,IC161*
RS	text	Seznam míst, na které má držitel rezervace, oddělených čárkou	RS:3-45,1-25*
SG	text	Podpis řetězce ETD, vygenerovaný podle popisu níže	SG:0123456789ABCDEFGHIJ KLMNOPQRSTUVWXYZ*

Zajištění a ověření pravosti

Vstupem pro výpočet elektronického podpisu je část řetězce ETD před samotným atributem podpisu, tj. hlavička a atributy v pořadí tak, jak jsou v těle ETD. Volitelně je tedy možné některé atributy z podpisu vyjmout jejich uvedením za atributem podpisu. Parametry použitého podpisu (hashovací funkci a eliptickou křivku) definuje vydavatel.

Generování podpisu ETD SG

1. Vypočte se hash z podepisované části ETD,
2. hash se zašifruje algoritmem ECDSA s použitím soukromého klíče vydavatele,
3. výsledek se převede do soustavy base32hex, odsekne se koncové bitové zarovnání (rovnítko) a
4. vloží jako hodnota atributu SG do ETD.

Ověření podpisu ETD SG

1. Vypočte se hash z ověřované části ETD,
2. hodnota klíče SG se doplní o bitové zarovnání (stejný počet rovnítek jako při sestavení),
3. převede ze soustavy base32hex na binární reprezentaci (pole bajtů),
4. dešifruje se algoritmem ECDSA s použitím veřejného klíče vydavatele a
5. výsledek se porovná s hashem z bodu 1.

Ověření platnosti

Pravidla pro úspěšné ověření platnosti ETD specifikuje vydavatel.

Zahrnuty by měly být minimálně tyto kroky:

- ověření syntaxe formátu ETD
- ověření identifikace vydavatele v atributu IN
- ověření pravosti podpisu v atributu SG (dle veřejného klíče vydavatele nebo všech platných klíčů, pokud atribut IN není přítomen nebo k němu nemá kontrolní aplikace přiřazen veřejný klíč)
- ověření hodnot atributů FR, TO, VS, VU, VL, VC, VZ (jsou-li uvedeny)
- zobrazení a manuální ověření hodnot atributů HN, HS, HI, RL, RS (jsou-li uvedeny)

Ukládání a sdílení

Pro potřeby přenosu ETD v protokolu HTTP či pomocí NFC je definován MIME type:

application/x-electronicticketdescriptor

Příklad

ETD*1*IN:DPP*VS:2018-06-19T10:15:00+02:00*VU:2018-06-19T10:30:00+02:00*VZ:1*TT:ADULT*TI:9
 82*SG:61304880NEMBL69BM8TQVBQEPCL80KR79GKQJHINR36K8IKEVJCRKU22MD104880VTM921DS6QTS4D287LN
 R6ST7SINMP0H6AN8NKLK7EVA4PQV5T7F0*X-TS:1G0D*

