České dráhy, a.s.
nábřeží L.Svobody 1222/12
Praha 1, 110 00

2D standard pro jízdní doklady ČD, a.s.

Základní pravidla a popis struktur

Odbor informatiky České dráhy, a.s.
Dne: 28.5.2012
Verze. 1.00

České dráhy, a.s.
nábřeží L.Svobody 1222/12
Praha 1, 110 00

1. Úvod

Dokument popisuje základní pravidla pro sestavení kontrolního kódu Aztec používaného na elektronických digitálně podepsaných jízdenkách. V této souvislosti se zde používá zkratka DST = Digitally Signed Ticket. Mezinárodní standardy, z nichž koncept vychází, jsou zakotveny v dokumentu TAP TSI: ANNEX B. 7: INTERNATIONAL RAIL TICKET FOR HOME PRINTING (vydavatelem je European Railway Agency).

2. Základní principy

Celý koncept vychází z těchto základních principů:

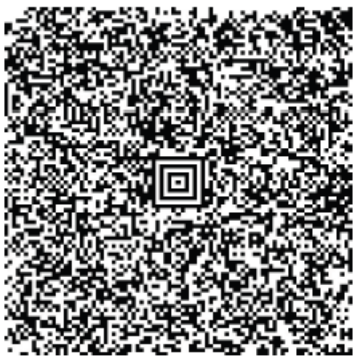
1. Data o jízdence jsou kódována jako binární data ve čtvercovém kódu dle normy Aztec.
2. Základní struktura dat je jasně dokumentovaná a i obecnou aplikací ji lze bez potíží načíst.
3. Součástí dat kódu je digitální podpis. Ten je vytvořen metodou DSA s použitím privátního klíče vydavatele DST. V ověření podpisu je třeba jeho veřejná část (certifikát). Takto lze s naprostou jistotou ověřit, že jízdenku skutečně vydala příslušná strana a že data nebyla následně žádným způsobem pozměněna.

3. 2D čárový kód

Toto je závazná specifikace použitého 2D čárového kódu:

parametr	hodnota	komentář
typ kódu	Aztec	
počet modulů	87 x 87	17 vrstev
kapacita	max. 621 bytů	data jsou zapsána binárně (8 bitů), limit nesmí být překročen, případně lze některé dílčí (volitelné) záznamy vynechat
velikost	50 x 50 mm	doporučená velikost pro tisk, zobrazení na displeji
minimální opravný kód	23 %	vyplývá z normy kódu Aztec

Příklad kódu dle uvedené specifikace:



3.1 Základní struktura dat kódu

Data kódu jsou členěna dle následující tabulky:

p. č.	prvek	počet bytů	kódování	komentář
1	Unikátní ID zprávy	3	A	železniční jízdenky zde mají „#UT“
2	Verze typu zprávy	2	N	železniční jízdenky zde mají „01“
3	RICS kód vydavatele	4	N	např. ČD je 1154
4	ID (párů) klíče	5	A	ID spravuje vydavatel DST
5	Podpis	50	A	DSA podpis zprávy po kompresi (prvky 6 a 7) dle ASN.1, jsou-li data po kompresi kratší než 50 byte, doplní se do počtu 50 nulovými byte
6	Délka komprimovaných dat	4	N	
7	Komprimovaná data	proměnlivé	A	algoritmus deflate, max. 553 bytů

Zde je jako příklad výpis výše uvedeného kódu. Modře jsou zde elementy p. č. 1 až 4, červeně je element 5 (podpis) a zeleně jsou vlastní data kódu (element 7, tj. délka komprimovaných dat má hodnotu 0410 bytů).

Počet bytů: **478 B**

Offs.	Data	Znaky
0000	23 55 54 30 31 31 31 35 34 54 54 30 30 31 30 2C	#UT011154TT0010,
0001	02 14 39 19 8B 4F D7 7A 28 3D 08 2A 82 B7 60 7E	..9..O.z(=.*..`~
0002	66 87 C4 F7 7C 17 02 14 2C 15 D4 D6 6B 3D F7 B0	f...|...,...k=..
0003	9E 90 E9 32 2D D0 49 17 FA D2 8A 5A 00 00 00 00	...2-.I....Z....
0004	30 34 31 30 78 9C 55 92 CF 6E DA 40 10 C6 7B CE	0410x.U..n.@..{.
0005	53 EC B9 72 E9 CC CE FE B1 B9 01 46 42 6C 5A 50	S..r.......FBlZP
0006	30 AA 92 4B 64 8A 25 48 A8 2D 39 7F A4 48 7D 05	0..Kd.%H.-9□H}.
0007	1E 20 CA 89 07 E8 23 B4 17 E3 F7 EA EC 22 13 65	. ....#.....".e
0008	2E 3F EB 5B CD E7 F9 76 76 79 3B 19 0F 52 40 00	.?.[...vvy;..R@.
0009	4D 88 5A 7D 06 40 F3 25 36 C9 A7 F7 42 0D 5A 02	M.Z}.@.%6...B.Z.
000A	4A 04 4C D4 68 91 8E 97 B7 D9 E5 E0 9A 9B C8 C2	J.L.h...........
000B	D5 28 93 DC 43 20 41 B3 A2 80 4B 79 27 16 25 10	.(..C A...Ky'.%.
000C	25 E0 1D A7 CD FE 26 1D 7F 77 83 8B 22 DB DE 17	%.....&..□w.."...
000D	8F E0 1D 09 FD 21 D8 8B D9 43 B5 12 08 86 FB 91	.....!...C......
000E	5D B8 34 EA 1E 7F 19 B0 67 05 A0 CF 30 6C 8A A1	].4..□.g...0l..
000F	0F 71 5E E7 9B 5C 6C 76 BD B2 07 86 54 A7 C3 B0	.q^..\lv....T...
0010	2E AB 4E F6 83 77 96 26 58 EA F8 AC 48 15 2C 8D	..N..w.&X...H.,.
0011	E9 14 36 8F 4F B1 FC 5C F1 BC 7D 2D 1E FA 62 BE	..6.O..\..}-..b.
0012	C9 2F 57 91 AB 76 CD 9F 32 72 93 AA CE 27 D1 E2	./W..v..2r...'..
0013	F9 F8 F6 B8 6B 0E 5F 17 D1 64 58 57 EB C8 B5 AF	....k._..dXW....
0014	DB F6 5F 5E 56 CF 51 B6 6D 0F 9E 7E 8E F6 EF 56	.._^V.Q.m..~...V
0015	B8 5F 7D 21 B5 F5 93 03 85 FF 48 39 5B BD 1C F7	._}!......H9[...
0016	C5 5D D9 1C C4 5D B1 2E AB F5 D3 CF 4D 73 40 D2	.]...]......Ms@.
0017	E7 78 72 54 94 B9 20 49 C2 1D F7 FE 42 97 19 84	.xrT.. I....B...
0018	0D B8 29 1F BA BC 2E 76 62 9A 97 C7 B7 7B 97 FA	..)....vb....{..
0019	D4 6E 04 90 A0 24 A5 8D 8D 13 E7 38 58 BA BC FA	.n...$.....8X...
001A	31 D4 6E 01 36 D1 4A 5B B0 E6 B7 27 9E 48 0A 95	1.n.6.J[...'.H..
001B	27 5F DC 89 48 14 28 D1 93 8D AC F6 34 94 04 52	'_..H.(.....4..R
001C	47 99 68 F7 0D 80 38 D3 8C 9F 8E 09 BB EA F9 17	G.h...8.........
001D	22 C2 92 D2 99 17 ED 47 F1 3F BA 70 9E AD	"......G.?.p..

3.2 Struktura dat DST po jejich rozbalení/před zabalením

Různorodý obsah zpráv vyžaduje flexibilní strukturu věty. Lze použít:

- obecné/univerzální typy záznamů, které jsou stejné pro všechny vydavatele DST EJD
- specifické typy záznamů dohodnuté mezi jednotlivými vydavateli

Každý typ záznamu je tvořen podle následujícího vzoru:

p. č.	prvek	počet bytů	kódování	komentář
1	ID záznamu	6	A	Uxxxxx pro standardizované záznamy TAP TSI, xxxxx je variabilní a určuje typ záznamu, nebo 4 znaky kódu vydavatele (ČD je 1154) + xx typy záznamu definované vydavateli
2	Verze záznamu	2	N	odlišuje různé verze jednoho typu záznamu se stejným ID
3	Délka záznamu	4	N	počet znaků záznamu (počítáno od prvního znaku ID záznamu)
4	…	…	…	vlastní obsah záznamu

3.2.1 Hlavní záznam (U_HEAD)

Tento záznam je povinný. Záznam obsahuje informace společné pro všechny typy jízdenek.

p. č.	prvek	počet bytů	kódování	komentář
1	ID záznamu	6	A	vždy „U_HEAD“
2	Verze záznamu	2	N	vždy „01“
3	Délka záznamu	4	N	
4	kód vydavatele DST	4	N	např. 1154 pro ČD
5	Jednoznačný kód jízdenky	20	A	určuje vydavatel, pro každý doklad musí být použit jednoznačný klíč, v kombinaci s kódem vydavatele je klíč jedinečnou identifikací DST jízdenky
6	Datum a čas vydání jízdenky	12	N	formát "DDMMYYYYHHMM" může být použit k eliminaci podvodů (např. nákup jízdenky během cesty)
7	Příznak	1	N	mezinárodní jízdenka = 1, vydáno agenturou = 2, vzor = 4, nastavení příznaků je věcí dohody vydavatelů
8	Jazyk dokladu	2	A	ISO 639-1 kód země
9	Druhý jazyk dokladu	2	A	ISO 639-1 kód země, není-li použit, je vyplněno nulami

3.2.2 Záznam dat jízdenky (U_TLAY)

Tento záznam je povinný. U mezinárodních jízdenek je nutné použít rozvržení podle normy RCT2. Tento záznam představuje úplnou informaci o uspořádání polí na tištěné jízdence tak, aby bylo možno provést úplnou kontrolu jízdenky bez on-line konektivity na prodejní systém. V záznamu by měla být obsažena pouze pole s proměnným obsahem. Pro kontrolu off-line je celý vzhled jízdenky extrahován z DST a zobrazen na displeji kontrolního zařízení. Zobrazený vzhled jízdenky by měl co nejpřesněji korespondovat s vytištěnou jízdenkou. Tento záznam se vztahuje pouze na obsah jízdenky, ne na konkrétní rozložení vzhledu dokladu (např. RCT 2). V důsledku toho i jízdenky, které nejsou standardizovány, mohou být takto zobrazovány.

p. č.	prvek	počet bytů	kódování	komentář
1	ID záznamu	6	A	vždy „U_TLAY“
2	Verze záznamu	2	N	vždy „01“
3	Délka záznamu	4	N	
4	Standard vzhledu	4	A	např. „RCT2“
5	Počet polí	4	N	počet za sebou následujících polí
Následující prvky definují jednotlivá textová pole, včetně popisu vzhledu jízdenky. Pro každé textové pole se prvky opakují (i = index textového pole)				
6 + 6i	Pole řádků	2	N	index řádku prvního písmene, od 0 do 14
7 + 6i	Pole sloupců	2	N	index sloupce prvního písmene, od 0 do 71
8 + 6i	Výška pole	2	N	počet řádků pole
9 + 6i	Šířka pole	2	N	počet sloupců pole
10 + 6i	Formátování pole	1	N	0 = normal, 1 = tučné, 2 = kurzíva, 3 = tučná kurzíva, 4 = malý font (132-font RCT2), 5 = malý font tučný, 6 = malý font kurzíva, 7 = malý font tučná kurzíva
11 + 6i	Délka textového pole	4	N	délka dále uvedeného textu (délka musí být stanovena na základě již kódovaného textu)
12 + 6i	Textové pole	n	A	je-li výška pole větší než 1, musí být text zalomen podle pravidel: • První slovo, které se nevejde do aktuálního řádku, je vytištěno na začátku následujícího řádku • Pokud textové pole obsahuje znak LF (ASCII "10"), další slovo musí být zalomeno do dalšího řádku vydavatel záznamu musí zaručit, že celý text, při uplatňování těchto pravidel, lze umístit a zobrazit v uvedených rozměrech pole (výška a šířka)

Poznámka: Při vytváření tohoto záznamu je třeba zohlednit, že piktogramy nelze použít v textovém poli. Pokud tištěná jízdenka obsahuje piktogramy, musí být tyto nahrazeny odpovídajícím textem.

Použití "malého fontu" nemá žádný vliv na počet znaků v daném poli. I při použití malého fontu je maximální šířka pole 71 znaků. Formátování "malý font" nelze použít pro zvýšení kapacity textového pole jízdenky.

3.3 Specifické typy záznamů jízdenky

Záznamy mohou obsahovat atributy DST, které nejsou definovány ve standardu TAP TSI. DST lze použít i pro vnitrostátní jízdenky, které neodpovídají normě TAP TSI. Pro tyto případy mohou vydavatelé definovat vlastní typy záznamů. Je třeba respektovat základní strukturu záznamu.

P. č.	prvek	počet bytů	kódování	komentář
1	ID záznamu	6	A	kód vydavatele pro první 4 znaky + ID (2 znaky určené vydavatelem)
2	Verze záznamu	2	N	
3	Délka záznamu	4	N	
4	…	…	…	vlastní obsah záznamu

3.4 Příklad

Zde je výpis záznamů z výše uvedeného příkladu.

Záznam U_HEAD, verze 01

Položka	Hodnota
Délka	0053 (data 41 B)
Vydavatel	1154
ID jízdenky	*0016-869
Datum a čas vydání	150520121019
Příznak	4 (test)
Jazyk	CS
Druhý jazyk	DE
Data	1154*0016-8691505201210194CSDE

Záznam U_TLAY, verze 01

Položka	Hodnota
Délka	0370 (data 358 B)
Vzhled	RCT2
Počet polí	0013
01 (05,02,04,01)	1154
02 (12,00,39,03)	JÍZDENKA eTiket
03 (52,00,19,03)	Osob 1
04 (01,06,05,01)	15.05
05 (07,06,05,01)	00:00
06 (12,06,19,01)	Praha hl.n.
07 (34,06,19,01)	Brno hl.n.
08 (52,06,05,01)	16.05
09 (58,06,05,01)	24:00
10 (66,06,05,01)	2
11 (01,08,70,03)	Přes: PhaLb,Kolín,KHoraH,Světlá/S,HBrod,Křižanov,Tišnov,BrnoŽi Km: 257
12 (01,12,50,03)	Obyčejná jednoduchá
13 (52,13,19,01)	Cena 323 Kč
Data	RCT2001302050104000041154001203390001 6JÍZDENKA*(LF)*eTiket0052031900007*(LF)*Osob 1060101050000515.05060701050000500:000612011900011Praha hl.n.0634011900010Brno hl.n.0652 01050000516.05065801050000524:000666010500001208010370000 78Přes: PhaLb,Kolín,KHo raH,Světlá/S,HBrod,Křižanov,Tišnov,BrnoŽi Km: 2571201035000022Obyčejná jednoduch á1352011900012Cena 323 Kč

Záznam 1154UT, verze 01

Položka	Hodnota
Délka	0194 (data 182 B)
KJ (jméno)	Karel Janěk

Položka	Hodnota
KD (druh průkazu)	0 (průkaz)
KC (číslo průkazu)	123456789
KK (kód transakce)	DURWB5
KS (směrování)	5457076|5457176|5453414|5454014|5454133|5454213|5434575|5436395|5433395|5433295
KM (km)	257
OD (platí od)	15.05.2012 00:00
DO (platí do)	17.05.2012 00:00
Data	KJ012Karel JaněkKD0010KC009123456789KK006DURWB5KS0795457076|5457176|5453414|5454014|5454133|5454213|5434575|5436395|5433395|5433295KM003257OD01615.05.2012 00:00DO01617.05.2012 00:00