

Elektronická kontrola vstupu

Doc. Ing. Karel Burda, CSc.



Program

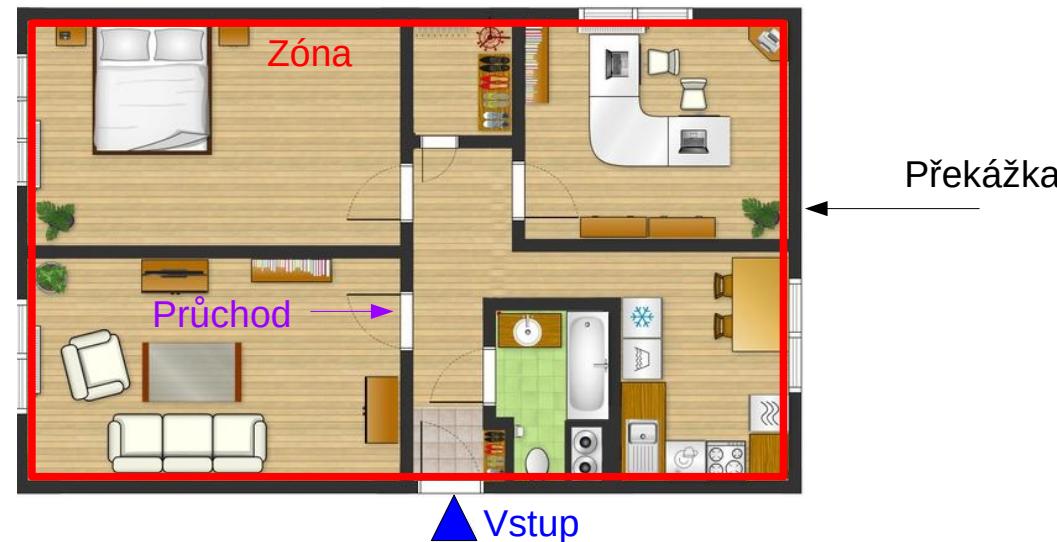
Elektronická kontrola vstupu (EKV)

1. Úvod
2. Architektura systémů EKV
3. Teorie autentizace
4. Autentizace hardwarem
5. Závěr

1. Úvod

Základní pojmy

- **Překážka**: materiální struktura, která znemožňuje pohyb osob do prostoru za touto překážkou. Obvykle se jedná o zed, nebo o plot.
- **Průchod**: prvek umístěný v překážce, který osobám umožňuje pohyb do prostoru za překážkou. Obvykle se jedná o stavební otvor bez výplně, či s nezamykanou výplní.
- **Vstup**: průchod opatřený pevnou uzavíratelnou výplní, který umožňuje pohyb za překážku pouze oprávněným osobám. Obvykle se jedná o zamykané dveře, nebo vrata.
- **Zóna**: část kontrolované oblasti, která je ohrazena překážkami a osoby se v ní mohou volně pohybovat. Zóna může být místnost, oplocený pozemek, ale také komplex místností navzájem propojených volně průchozími průchody, tak jak to je na obrázku.



EKV versus docházkový systém

- Elektronická kontrola vstupu (EKV) alias přístupový systém je elektronický systém určený k automatizovanému řízení vstupů v kontrolované oblasti.
 - V Evropě se používá název „Electronic Access Control System“ (EACS), v Severní Americe se spíše potkáme s označením „Physical Access Control System“ (PACS).
 - Příbuzným systémem k přístupovému systému je docházkový systém.
 - Docházkový systém je systém určený k evidenci přítomnosti osob v prostorách patřících dané organizaci. Z technického hlediska se jedná o speciální případ systému EKV, kde nejsou použity vstupy. Účelem tohoto systému totiž není omezování pohybu osob v prostorech organizace, ale evidence přítomnosti a pohybu těchto osob.



Řízení přístupu (1/2)

- **Přístupová politika:** stanovení, **kdo** a **kdy** může ve které **zóně** pobývat.
- **Autorita:** osoba, která stanovuje přístupovou politiku organizace.
- **Autorizace:** jednorázový akt přiřazení identity, práv a autentizačních faktorů. Autorita v rámci autorizace každé osobě X obecně přiřazuje:
 - unikátní **identifikátor** osoby (ID_x),
 - **přístupová práva:** ve které době smí osoba do kterých zón vstupovat (PR_x),
 - **dokazovací faktor** (DF_x): **něco**, čím bude osoba X přístupovému systému dokazovat svoji identitu (např. heslo, tajná data v kartě, nebo otisk prstu - viz obrázky),
 - **ověřovací faktor** (OF_x): **data**, s jejichž pomocí bude přístupový systém ověřovat skutečnost, že prověřovaná osoba disponuje dokazovacím faktorem osoby X.
- **Nosič faktoru:** materiální struktura, z níž lze DF, resp. OF přečíst.
- Nosičem dokazovacího faktoru (**NDF**) může být samotná osoba nebo vhodný předmět.
- Nosičem ověřovacího faktoru (**NOF**) je paměťové úložiště přístupového systému.



Řízení přístupu (2/2)

- Do systému EKV musí autorita vložit přístupový seznam a ověřovací seznam.
- **Přístupový seznam** obsahuje pro každou ze všech N autorizovaných osob **identifikátor ID** osoby a **práva PR** přidělená dané osobě (tj. které vstupy a kdy smí daná osoba využívat). Systém EKV podle tohoto seznamu zjišťuje přístupová práva osob.
- **Ověřovací seznam** obsahuje pro každou osobu její **ID** a ověřovací faktor **OF**. Tento seznam je potřebný k autentizaci žadatelů (viz dále).
- **Identifikace** je **zjištění identity** (tj. ID) osoby.
- **Autentizace** je **ověření identity** osoby.
- Metody autentizace:
 - **s oznámením**: při přístupu osoba X **uveďe** svůj identifikátor ID_x . V ověřovacím seznamu se nalezne **příslušný OF_x** a pomocí **autentizačního testu** se ověří, zda žadatel o vstup disponuje dokazovacím faktorem osoby s identifikátorem ID_x . Tato metoda se používá v **počítačích**.
 - **s rozpoznáním**: osoba svůj **identifikátor neuvádí**, čímž se autentizace stává rychlejší. Podle ověřovacího seznamu se postupně **zkouší** jednotlivé ověřovací faktory. Pokud je autentizační test úspěšný pro ověřovací faktor osoby s ID_x , tak se potom žadatel považuje za osobu X. V systémech **EKV** se z důvodu zrychlení autentizace používá výhradně tato metoda.
- Shrňme-li to, tak systém EKV pomocí ověřovacího seznamu provede nejprve **autentizaci** žadatele (tj. zjistí si jeho identitu) a poté z přístupového seznamu **zjistí práva** žadatele. Podle nich je vstup buď **otevřen**, nebo zůstane i nadále blokován.

Vývoj systémů EKV

- Až do **60. let** minulého století byl dokazovacím faktorem **klíč k zámku**. Uvedená metoda však byla nákladná (při ztrátě klíče musel být vyměněn zámek) a byla i málo operativní.
- V **70. letech** se dokazovacím faktorem stala znalost **tajného hesla** (tzv. PIN). Osoba jednoduše pomocí klávesnice u dveří předala systému svoje heslo. Nevýhodou bylo pomalé vkládání hesel a chyby při vytíkání hesla.
- V **80. letech** dominovaly jako nosič dokazovacího faktoru **Wiegandovy karty**. Osoba protažením karty ve čtečce u dveří předala systému tajná data ve své kartě (tzv. Wiegandovo slovo WS). Došlo tím ke zrychlení autentizace, ale časem bylo snadné tyto karty klonovat.
- V **90. letech** došlo k nástupu **paměťových karet** (Proximity card). Osoba přiložením karty ke čtečce předala systému tajná data ve své kartě (opět Wiegandovo slovo WS). Ale i tyto karty se nakonec staly snadno klonovatelné.
- Na **začátku 21. století** se začaly používat **biometrika osob** a **mikropočítáčové karty** (Smart card).
- V případě **biometriky** si osoba nechá čtečkou u dveří změřit svoji biometriku, což jsou unikátní morfologické, nebo behaviorální **rysy osob** (např. tvar papilárních linií prstů nebo způsob chůze). Tyto rysy jsou dokazovacím faktorem osoby.
- V případě **mikropočítáčové karty** je dokazovacím faktorem **kryptografický klíč** uložený v kartě. Přiložením karty ke čtečce se spustí kryptografický protokol, v jehož rámci si čtečka ověřuje, zda karta má k dispozici správný tajný klíč.

2. Architektura systémů EKV

Základní prvky systému EKV

- **Kontrolér** (obr. A): řídící jednotka přístupového systému.
- **Vstup** (obr. B): uzavíratelný průchod, který je elektricky ovládán kontrolérem. Obvykle se jedná o dveře s elektrickým otvíračem.
- **Terminál** (obr. C): zařízení pro komunikaci osoby s přístupovým systémem. Obvykle se jedná o čtečku biometriky (např. otisku prstu), čtečku karet, klávesnici pro vložení hesla nebo případně nějakou kombinaci uvedených zařízení.
- **Správní jednotka** (obr. D): zařízení pro správu přístupového systému. Obvykle se jedná o počítač se specializovaným softwarem.

A) Kontrolér



B) Vstup



C) Terminál



D) Správní jednotka



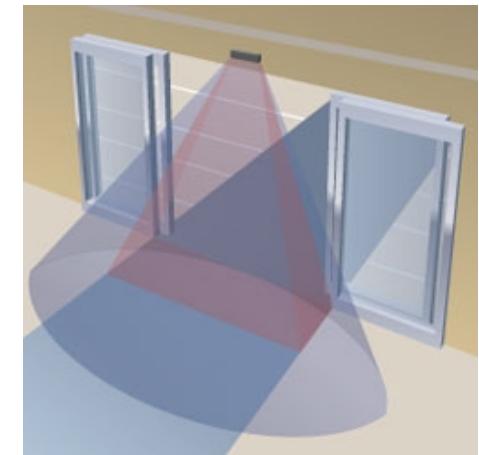
Vstupy

- **Vstup** je uzavíratelný průchod, který je elektricky ovládán kontrolérem. Po úspěšné autentizaci je uzavíratelná výplň průchodu kontrolérem **krátkodobě odblokována**, takže oprávněná osoba může vstoupit do kontrolovaného prostoru za vstupem.
- K řízení přístupu **osob** se jako vstupy používají obvykle dveře a turnikety.
- **Turniket** (obr. vlevo a uprostřed) je zábrana, která umožňuje průchod výhradně po **jednotlivých** osobách.
- K řízení přístupu **vozidly** se obvykle používají brány, závory a zásuvné sloupy.
- **Zásuvné sloupy** (obr. vpravo) jsou odolné, kovové sloupy, které lze hydraulicky zasunout na úroveň vozovky. Ve vysunuté poloze brání volnému průjezdu vozidel.



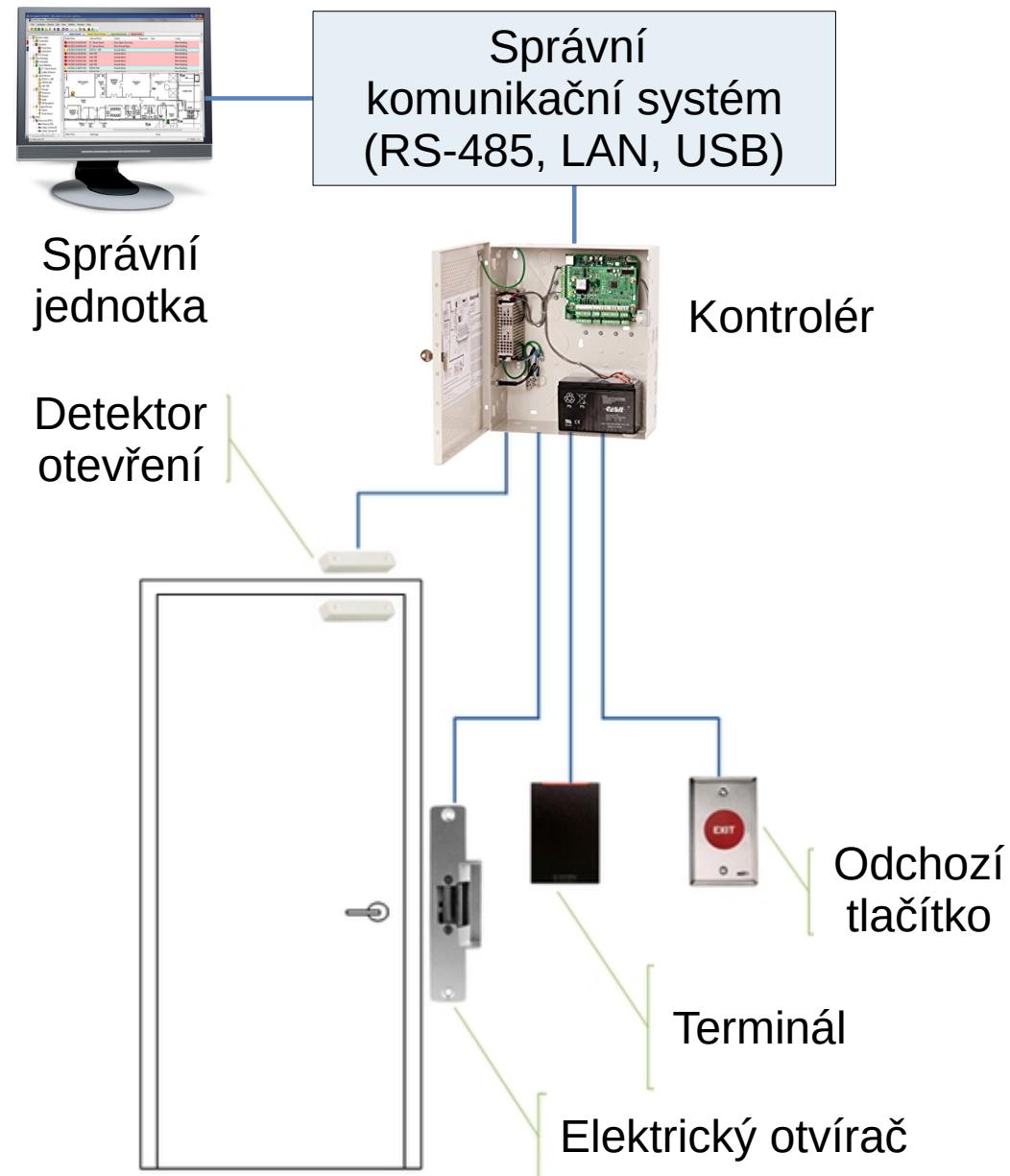
Další prvky systému EKV

- Kromě **kontroléru, vstupu, terminálu** a **správní jednotky** bývá součástí systému EKV i detektor otevření a odchozí tlačítko.
- **Detektor otevření** (obr. vlevo) známe z PZS. V EKV se používá k detekci neoprávněného otevření vstupu a k detekci stavu, kdy vstup není uzavřen. Pokud jsou dveře otevřeny bez povolení kontroléru, tak kontrolér vyhlásí poplach. Pokud nejsou po povoleném průchodu osoby dveře do stanovené doby zavřeny, tak je rovněž vyhlášen poplach.
- **Odchozí tlačítko** (obr. uprostřed) nahrazuje v kontrolované zóně terminál. Osoba si jeho stiskem vyžádá od kontroléru otevření vstupu pro svůj odchod z kontrolované zóny. Někdy se odchozí tlačítko nahrazuje **detektorem pohybu** MW nebo PIR. Detekční diagram detektoru pokrývá blízké okolí vstupu (obr. vpravo). Pokud osoba do této oblasti vstoupí, tak to detektor detekuje a kontrolér vstup automaticky otevře.



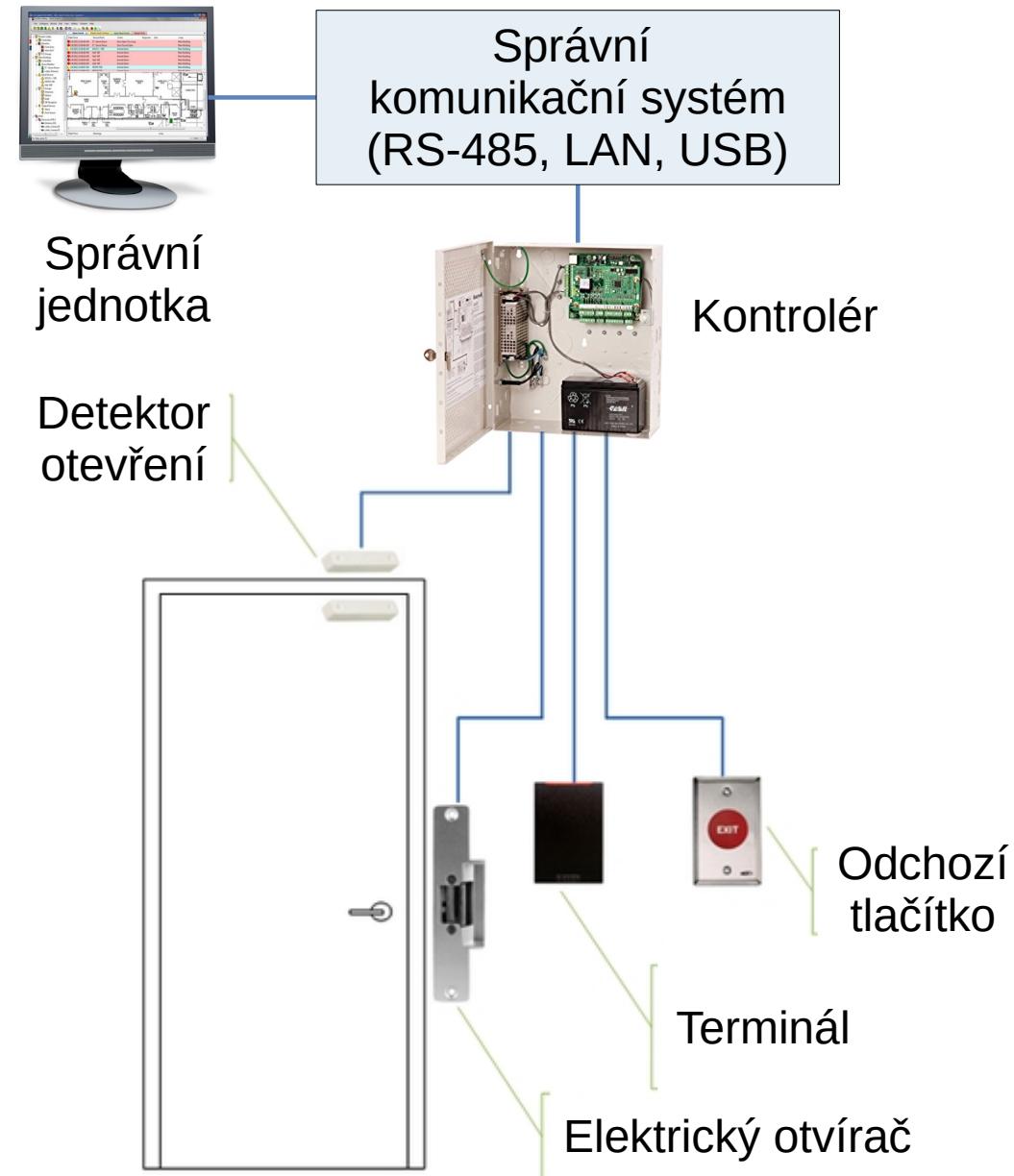
Obecná architektura systému EKV

- **Kontrolér** je ústřední prvek, na který se připojují všechny ostatní prvky systému.
- **Správní jednotka** slouží k aktualizaci přístupového a ověřovacího seznamu systému EKV. Ke kontroléru se připojuje buď lokálně (typicky přes USB či RS-232) nebo vzdáleně (typicky přes sběrnici RS-485 či přes LAN).
- **Výpočetně náročnou** autentizaci osob neprovádí kontrolér, ale terminál. K aktualizaci jeho ověřovacího seznamu se proto musí být správní jednotka schopna připojit nejen ke kontroléru, ale i k terminálu (obvykle pomocí sítě LAN).
- **Terminál** se ke kontroléru obvykle připojuje pomocí pěti i vícežilového rozhraní Wiegand.
- **Ostatní** prvky jsou ke kontroléru obvykle připojeny dvoudrátovou smyčkou.



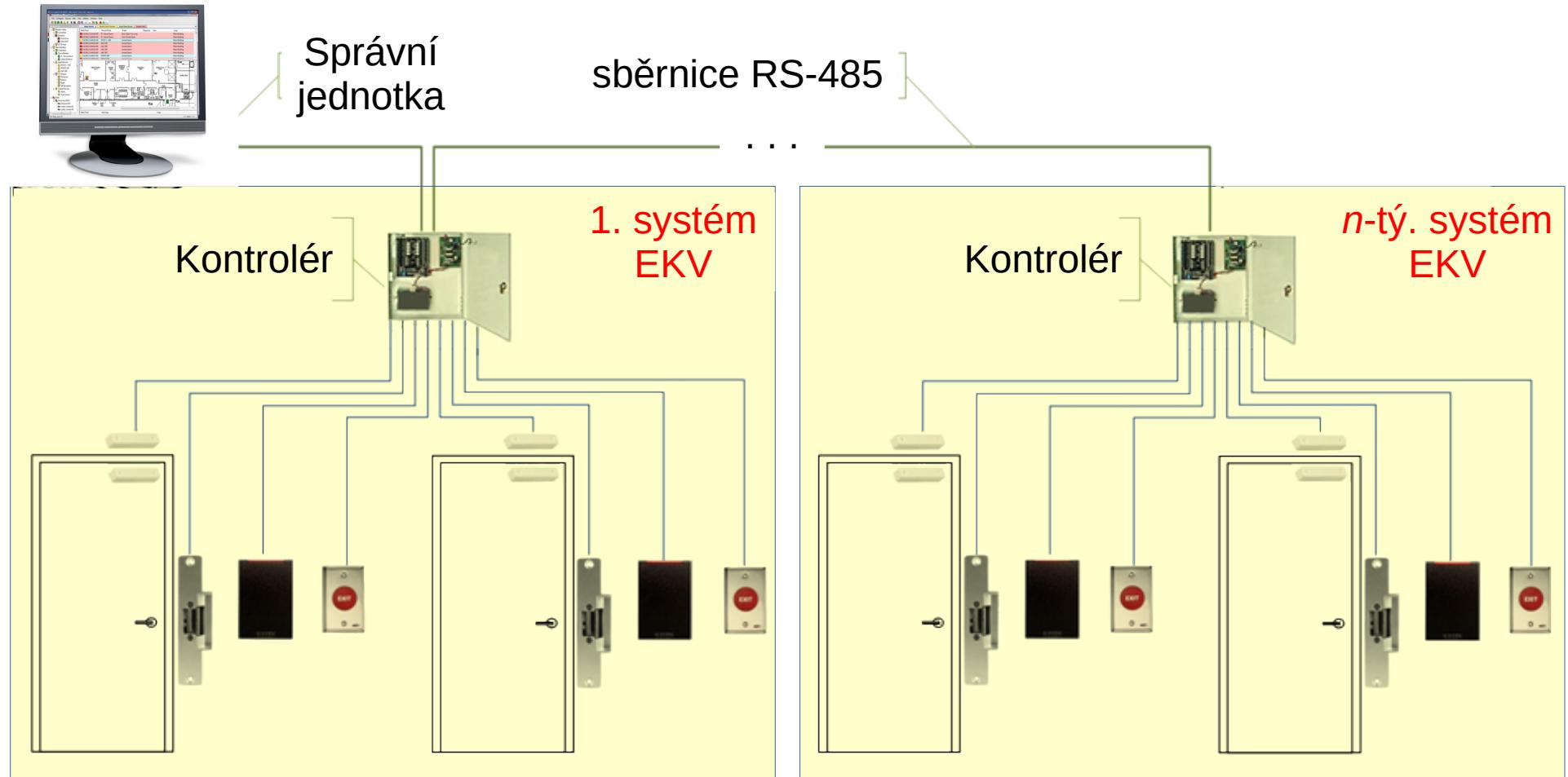
Fungování systému EKV

1. Před zahájením samotného provozu vloží autorita pomocí správní jednotky do systému přístupový a ověřovací seznam.
2. V rutinném provozu se žadatel o přístup prostřednictvím terminálu autentizuje.
3. Pro zjištěnou identitu vyhledá kontrolér v přístupovém systému práva žadatele.
4. Na základě zjištěných práv kontrolér pomocí elektrického otvírače buď vstup odemkne, nebo jej ponechá ve stavu zamčeno.
5. Detektor otevření detekuje násilné otevření vstupu nebo stav, kdy žadatel za sebou vstup nezavřel.
6. Odchozí tlačítko se instaluje v kontrolované zóně (stejně jako kontrolér a detektor otevření) a osoba si jím vyžaduje otevření vstupu při odchodu.



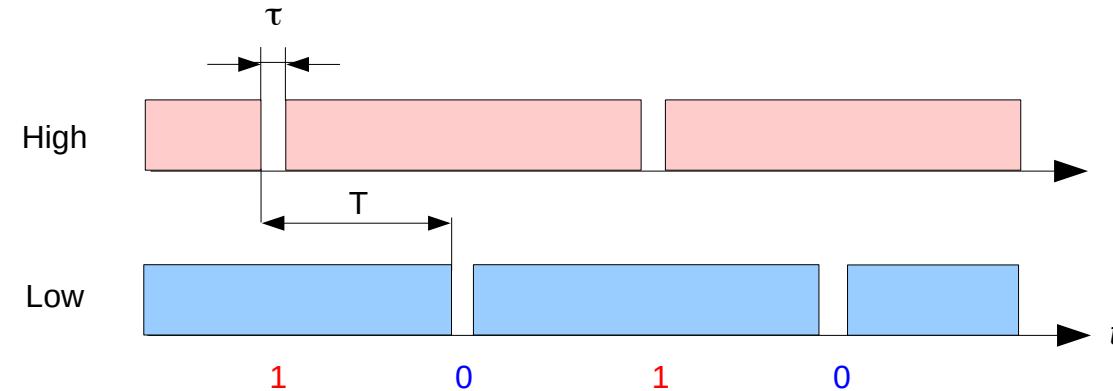
Obvyklé řešení rozsáhlého systému EKV

- **Kontrolér** obvykle řídí dva vstupy. Pokud je zapotřebí řídit více vstupů, tak se vytvoří n autonomních systémů EKV s centralizovanou správou přes sběrnici RS-485 nebo síť LAN.



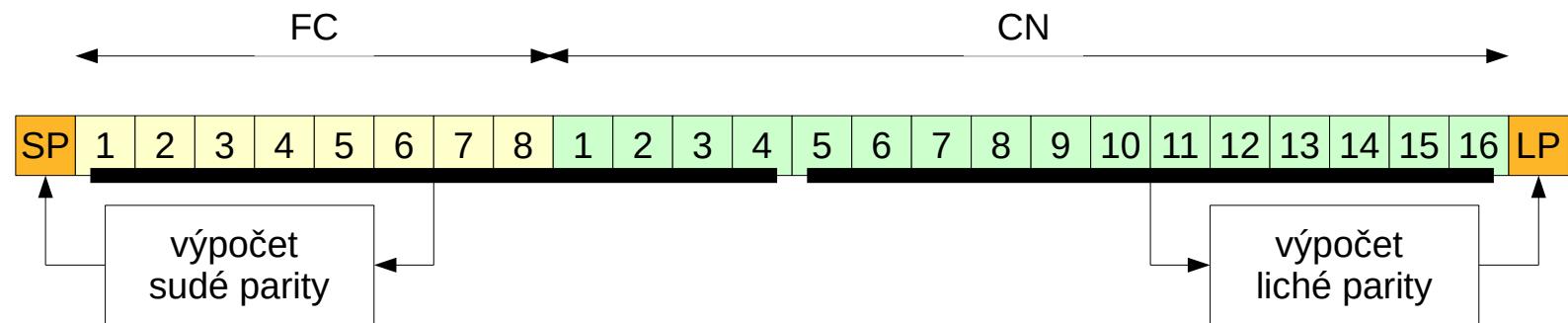
Rozhraní Wiegand

- Rozhraní Wiegand je standardní rozhraní pro jednosměrný přenos dat od terminálu ke kontroléru.
- Obvykle sestává z pěti vodičů:
 - Napájení: napájecí napětí pro terminál,
 - Zem: společná pro napájení i ostatní vodiče,
 - High: pro přenos jedničkových bitů,
 - Low: pro přenos nulových bitů,
 - Ovládání: rozsvícením diody LED kontrolér indikuje žadateli povolení ke vstupu.
- Data se přenášejí jen směrem od terminálu ke kontroléru. Klidový stav na vodičích High a Low je +5 V. Logická 1, resp. 0 je reprezentována krátkodobou ztrátou napětí na vodiči High, resp. Low, přičemž doba τ může být v rozsahu 20 až 100 μ s. Odstup mezi těmito negativními pulzy je doba T v rozsahu hodnot 200 μ s až 20 ms.
- Příklad přenosu bitů 1010:



Wiegandovo slovo

- **Wiegandovo slovo**: standardní identifikátor osob v systémech EKV.
- Wiegandovo slovo má obvyklou délku 26 bitů se strukturou podle obrázku.
- Sekvence bitů **FC** 1 až FC 8 („Facility Code“) je **identifikátorem organizace** a posloupnost bitů **CN** 1 až CN 16 („Card Number“) je **číslo karty** v dané organizaci.
- Bit **SP** je **paritní bit** první poloviny slova, tj. bitů FC 1 až FC 8 a CN 1 až CN 4. Bit **LP** je **paritní bit** druhé poloviny slova, tj. bitů CN 5 až CN 16.
- Bit **SP** se vypočítává technikou **sudé parity** a bit **LP** technikou **liché parity**.
- Identifikátor organizace **FC** má délku **pouze 8 bitů**, takže lze definovat jen $2^8 = 256$ organizací. To je pro unikátní identifikaci z celoplanetárního hlediska velmi málo a proto osoby z různých organizací mohou mít přidělenu kartu se stejným Wiegandovým slovem, tj. mohou mít stejný identifikátor. Z tohoto důvodu výrobci systémů EKV definovali další identifikační slova o větší délce než 26 bitů (např. 34 nebo 37 bitů).



3. Autentizace

Typy autentizace

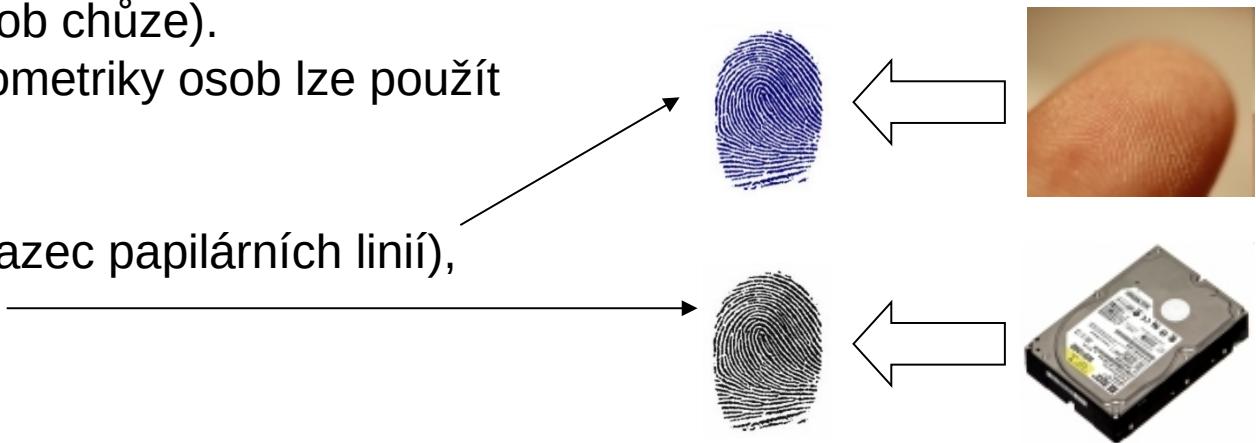
- Typy autentizace lze klasifikovat podle kombinace dokazovacího faktoru (DF) a nosiče dokazovacího faktoru (NDF):
 - nosič DF je **osoba**:
 - DF = **tajná data** (obvykle PIN, nebo heslo),
 - DF = **biometrika osoby** (nepadělatelné rysy osoby jako je např. otisk prstu),
 - nosič DF je **předmět**:
 - DF = **tajná data** (obvykle Wiegandovo slovo, nebo kryptografický klíč),
 - DF = **nepadělatelné rysy předmětu** (mikrotext, reliéfy či holografické fólie).
- Potom nejobvyklejší metody autentizace můžeme charakterizovat následovně:
 - autentizace **biometrikou**: NDF = osoba, DF = biometrika osoby,
 - autentizace **heslem**: NDF = osoba, DF = tajná data uložená v paměti osoby (PIN),
 - autentizace **průkazem**: NDF = předmět, DF = nepadělatelné prvky předmětu (průkaz),
 - autentizace **hardwarem**: NDF = předmět, DF = tajná data uložená v předmětu (karta).

Nosič dokazovacího faktoru

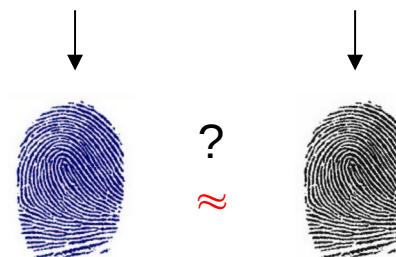
Dokazovací faktor		
	Osoba	Předmět
Rysy	Biometrika	Průkaz
Data	Heslo	Hardware

Autentizace biometrikou (1/2)

- Biometriky jsou **kvantifikovatelné** rysy osoby. Buď se jedná o:
 - morfologii** osoby (např. obrazec papilárních linií),
 - chování** osoby (např. způsob chůze).
- Unikátní** a nepadělatelné biometriky osob lze použít k jejich autentizaci.
- V tomto případě platí:
 - DF = biometrika (např. obrazec papilárních linií),
 - OF = datový záznam DF.



- Při autentizaci se vhodným snímačem sejme obraz biometriky osoby. Tato tzv. **dokazovací data (DD)** jsou předána autentizátoru.
- Kritérium úspěšné autentizace: DD \approx OF.



Symbol „ \approx “ vyjadřuje skutečnost, že záznam biometriky (tj. OF) nebývá zcela shodný s aktuálně sejmutou biometrikou (tj. DD).

Autentizace biometrikou (2/2)

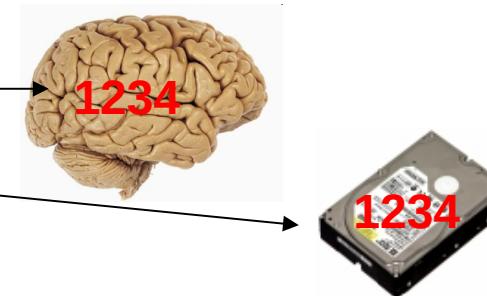
- Již jsme uvedli, že v systémech EKV žadatelé o přístup **neuvádějí** svůj identifikátor ID, tj. autentizuje se metodou **rozpoznávání**. Důvodem je minimalizace doby trvání autentizace a tedy maximalizace propustnosti vstupů.
- U biometrické autentizace se pro aktuální dokazovací data DD postupně **testují** ověřovací faktory OF osob v ověřovacím seznamu. Pokud platí, že $DD \approx OF_x$, tak se žadatel považuje za osobu **X**.
- Pokud **N** je počet autorizovaných osob v ověřovacím seznamu, tak se při autentizaci žadatele musí v průměru provést **(N+1)/2** autentizačních testů. Soudobé biometrické autentizátory mají kapacitu **N** řádově tisíců osob s průměrnou dobou autentizace do 1 s.
- Biometrickou autentizaci obvykle neprovádějí kontroléry, ale provádějí ji **terminály**. Osoba si snímačem terminálu nechá **sejmout** biometriku (DD) a terminál podle ověřovacího seznamu zjistí identifikátor **ID** žadatele. Zjištěný identifikátor (obvykle Wiegandovo slovo WS) **zašle** **kontroléru**, který pak podle přístupového seznamu ovládá vstup.
- **Správní jednotka** aktualizuje ověřovací seznamy **terminálů** obvykle pomocí kryptograficky zabezpečeného spojení přes počítačovou **IP síť**.
- **Výhody**: žadatel má DF stále sebou.
- **Nevýhody**:
 - terminály pro autentizaci biometrikou jsou poměrně drahé,
 - dokazovací faktory nejsou tajné. Útočník je může zjistit a vyrobit padělek.

Autentizace heslem (1/2)

- Autentizace heslem je založena na znalosti **hesla**, což je tajný a **zapamatovatelný** řetězec znaků. V systémech EKV se heslo obvykle nazývá **PIN** („Personal Identification Number“).

- V tomto případě platí:

- DF = PIN,
- OF = DF,
- DD = DF.



- Při autentizaci osoba pomocí klávesnice terminálu vloží heslo, tj. **dokazovací data DD**.
- Kritérium úspěšné autentizace: DD = OF.

$$\begin{array}{c} \downarrow & ? & \downarrow \\ 1234 & = & 1234 \end{array}$$

Autentizace heslem (2/2)

- Autorita při autorizaci přidělí osobě doposud nepoužitou hodnotu PIN, která plní funkci jak tajného DF, tak i ID a OF. To znamená, že **PIN = ID = DF = OF**.
- Žadatel vloží do systému prostřednictvím numerické klávesnice terminálu svá dokazovací data **DD = PIN**. Terminál hodnotu DD předá kontroléru.
- Autentizaci provádí **kontrolér**. Ten hodnotu DD hledá ve sloupci ID přístupového seznamu (viz obrázek). V řádku, který přísluší hodnotě PIN, pak nalezne práva PR žadatele.
- Protože PIN je zároveň DF, tak tím **zároveň** kontrolér provedl autentizaci.
- Platí totiž, že při délce n číslic je počet všech hodnot pinu $M = 10^n$.

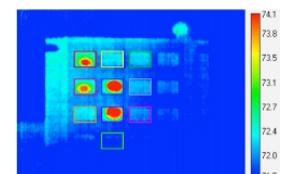
Pokud počet autorizovaných žadatelů $N \ll M$, tak je nepravděpodobné, že případný útočník vloží jednu z N správných hodnot. Správnou hodnotu je schopna vložit jen autorizovaná osoba.

- **Výhody**: velmi jednoduché a laciné.

- **Nevýhody**:

- osoba svůj DF zapomene,
- variabilita DF není velká, protože DF musí být zapamatovatelný. Útočník pak může aplikovat tzv. **slovníkový útok**, kdy bude postupně zkoušet možná hesla.
- útočník může také vkládané heslo odpozorovat, nebo odhadnout pomocí parazitního kanálu (např. tepelná stopa na použitých klávesách – viz obrázek).

ID	PR
PIN_1	PR_1
PIN_2	PR_2
...	...
PIN_N	PR_N



Autentizace průkazem (1/2)

- V případě autentizace průkazem je identita osoby uvedena na **nepadělatelném** předmětu, tzv. průkazu (obr. vlevo).
- Ověřovatel nejprve pomocí ochranných prvků zkонтroluje, zda **není** průkaz padělán. Pokud je vše v pořádku, tak důvěruje údajům o identitě osoby, které jsou na průkazu uvedeny.
- V tomto typu autentizace platí:
 - DF = nepadělatelné **ochranné prvky** průkazu,
 - OF = znalost **ochranných prvků** průkazu (viz obrázek vpravo).
- Kritérium úspěšné autentizace: průkaz není modifikován, ani padělán.



Ochrannými prvky průkazů jsou různé **hologramy**, symboly viditelné pod **UV** světlem, symboly s **jinou** barvou podle úhlu pozorování apod.

- **Výhody:** ověřovatelem může být člověk, který se může obejít bez jakékoliv techniky.
- **Nevýhody:**
 - uživatel DF ztratí, nebo je mu ukraden,
 - drahé kvůli ochranným prvkům a pro elektronickou autentizaci nepoužitelné.

Autentizace průkazem (2/2)

- Autentizace průkazem se v praxi používá v přístupových systémech, kde autentizátorem je osoba (např. člen ostrahy objektu). V elektronických systémech se tento způsob autentizace nepoužívá, protože technologie pro strojové ověření pravosti průkazů jsou nákladné.
- V případě průkazů se často setkáváme s tzv. dvoufaktorovou autentizací, kdy je osoba ostrahou autentizována dvěma technikami a to průkazem a biometrikou.
- Průkaz je v takovémto případě opatřen také fotografií autorizované osoby. Tato fotografie je prakticky ověřovací faktor OF, který v průkazu zasílá autorita ostraze objektu. Člen ostrahy nejprve ověří pravost průkazu (tím si zároveň potvrdí pravost fotografie) a následně podle této fotografie ověří shodu obličeje osoby s fotografií. Tím prakticky provede biometrickou autentizaci držitele průkazu podle obličeje.
- Podle ID osoby, které je v průkazu uvedeno, pak člen ostrahy zjistí v přístupovém seznamu práva osoby a na základě nich rozhodne, zda žadatele do objektu vpustí či nikoliv.



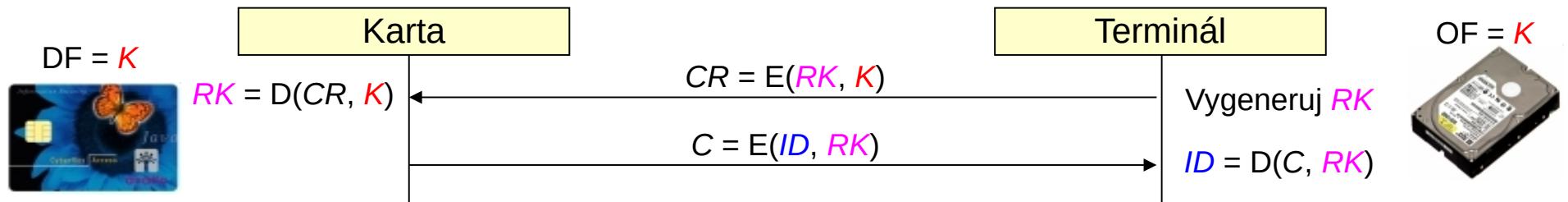
Autentizace hardwarem – paměťové úložiště

- Autentizace hardwarem je založena na **tajných datech** uložených v předmětu. Data tak mohou mít větší (tj. osobou **nezapamatovatelnou**) délku.
- Předmět může být buď **paměťové úložiště**, nebo **mikropočítač**. Tyto předměty komunikují s terminálem obvykle pomocí vhodného **bezdrátového rozhraní**.
- V případě paměťového úložiště je dokazovacím faktorem DF unikátní číslo, nejčastěji tzv. **Wiegandovo slovo WS**, jehož délka je typicky 26 bitů.
- V případě paměťového úložiště platí, že **WS = DF = OF = ID**.
- Žadatel přiblíží paměťové úložiště k terminálu, čímž zahájí bezdrátovou komunikaci mezi terminálem a úložištěm. V jejím rámci terminál zjistí **DD = WS**, které předá kontroléru.
- Kontrolér postupuje podobně jako v případě autentizace heslem, tj. hodnotu DD vyhledá v přístupovém seznamu ve sloupci ID. V řádku, kde ID = WS pak nalezne práva žadatele.
- Protože WS je zároveň DF, tak tím **zároveň** kontrolér provedl autentizaci – jen osoba s ID = WS může mít úložiště s tajným dokazovacím faktorem DF = WS.

- **Výhody**: relativně laciné.
- **Nevýhody**: uživatel úložiště s DF ztratí, nebo je mu ukradeno.

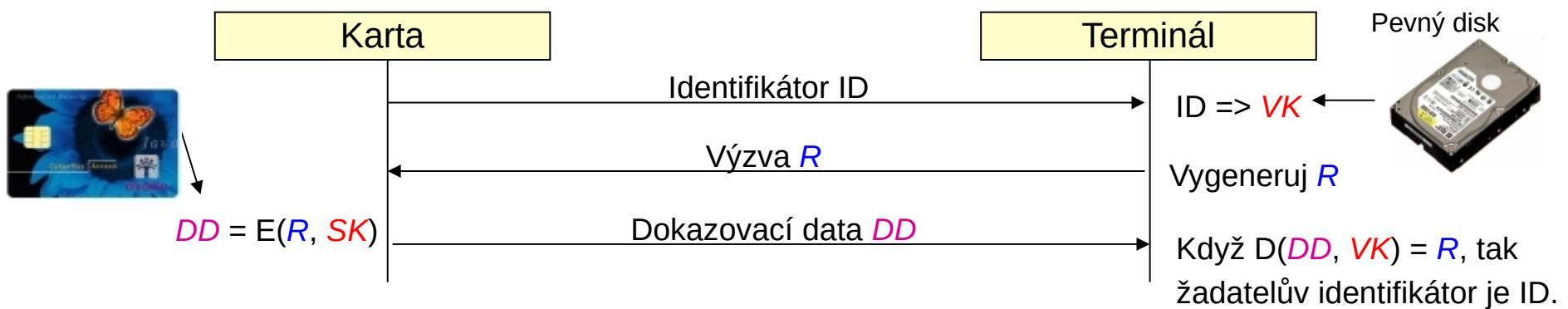
Autentizace hardwarem – mikropočítač (1/2)

- Autentizace pomocí mikropočítače je založena na kryptografii. Dokazovacím faktorem je **tajný klíč** uložený v kartě.
- Obvykle se využívá symetrická kryptografie, ale prosazuje se i asymetrická kryptografie.
- V případě **symetrické kryptografie** je dokazovacím a zároveň ověřovacím faktorem **tajný klíč K**. Platí tedy, že $DF = OF = K$. Tento klíč je obvykle platný pro celou organizaci, tj. disponují jím všechny čtečky a všechny karty dané organizace (např. firmy).
- Nejprve terminál a karta naváží bezdrátovou komunikaci.
- Princip autentizačního protokolu je takový, že terminál vygeneruje náhodný **relační klíč RK** a odešle jej jako kryptogram $CR = E(RK, K)$, kde **E** je operace **šifrování**. Karta **dešifrováním D** získá $RK = D(CR, K)$.
- Karta poté relačním klíčem zašifruje identifikátor **ID** žadatele (obvykle Wiegandovo slovo) a kryptogram $C = E(ID, RK)$ odešle terminálu. Ten jej dešifruje a získá $ID = D(C, RK)$. Hodnotu **ID** poté zašle kontroléru.
- Kontrolér podle **ID** zjistí přístupová práva žadatele a podle toho vstup otevře, resp. neotevře.



Autentizace hardwarem – mikropočítač (2/2)

- V případě **asymetrické kryptografie** se používají dvojice klíčů. Jeden z dvojice je tajný (tzv. **soukromý klíč SK**) a druhý je veřejně známý klíč (tzv. **veřejný klíč VK**). Ze znalosti VK přitom **nelze** určit hodnotu SK. Autorita ani systém tak **nepotřebují znát DF uživatelů**.
- U autentizace v systémech EKV platí, že **DF = SK** a **OF = VK**. Autentizační protokol může fungovat následovně.
- Nejprve terminál a předmět naváží bezdrátovou komunikaci. Předmět oznámí **ID** žadatele.
- Terminál odešle náhodné číslo **R** (tzv. **výzvu**). Předmět výzvu **zašifruje** (operace **E**) pomocí klíče **SK**. Vzniklá **dokazovací data DD = E(R, SK)** odešle terminálu.
- Terminál v ověřovacím seznamu **vyhledá** pro oznámené ID klíč **VK**. Tímto klíčem přijatá **DD dešifruje** (operace **D**). Pokud pak platí, že **D(DD, VK) = R**, tak žadatel má předmět, kterým má disponovat osoba s oznámeným ID. Hodnotu ID poté zašle kontroléru.
- Kontrolér zjistí přístupová práva žadatele ID a podle toho vstup otevře, resp. neotevře.



Autentizace v systémech EKV - shrnutí

- Již jsme uvedli, že v systémech EKV se autentizace pomocí průkazu **nepoužívá**, protože by byla drahá. Vyplývá to z toho, že každý typ takové autentizace (např. ověření pravosti bankovky) vyžaduje speciální měřící zařízení a postupy (např. vyhodnocení grafických obrazců pod UV ozářením).



- V **praxi** se tak u systémů EKV potkáme s autentizací na základě:
 - **hesla** (obvykle PIN),
 - **biometriky** (např. otisk prstu),
 - vlastnictví **hardwaru** (např. čipové karty).
- K vyšší bezpečnosti se tyto autentizace kombinují (tzv. **vícefaktorová** autentizace):
 - **dvoufaktorová** autentizace (zpravidla PIN+hardware nebo PIN+biometrika),
 - **třífaktorová** autentizace (PIN+hardware+biometrika).

4. Autentizace hardwarem

Autentizační hardware

- K autentizaci v systémech EKV se jako autentizační hardware používá:
 - paměťová úložiště (zleva doprava):
 - karta s magnetickým proužkem,
 - Wiegandova karta,
 - RFID karta (neboli „Proximity Card“),

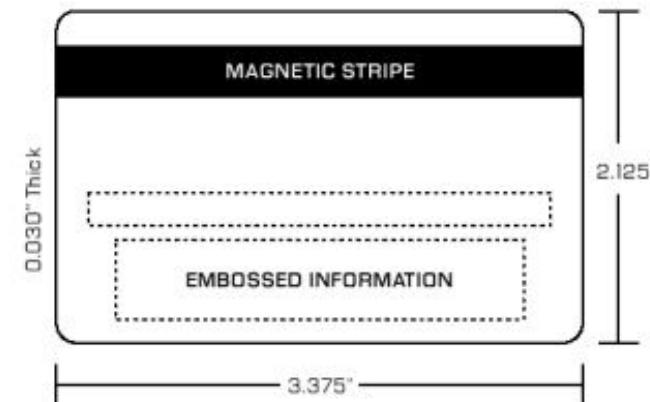


- mikropočítače (zleva doprava):
 - mikroprocesorová karta (neboli „Smart Card“),
 - smartfon.



Karta s magnetickým proužkem

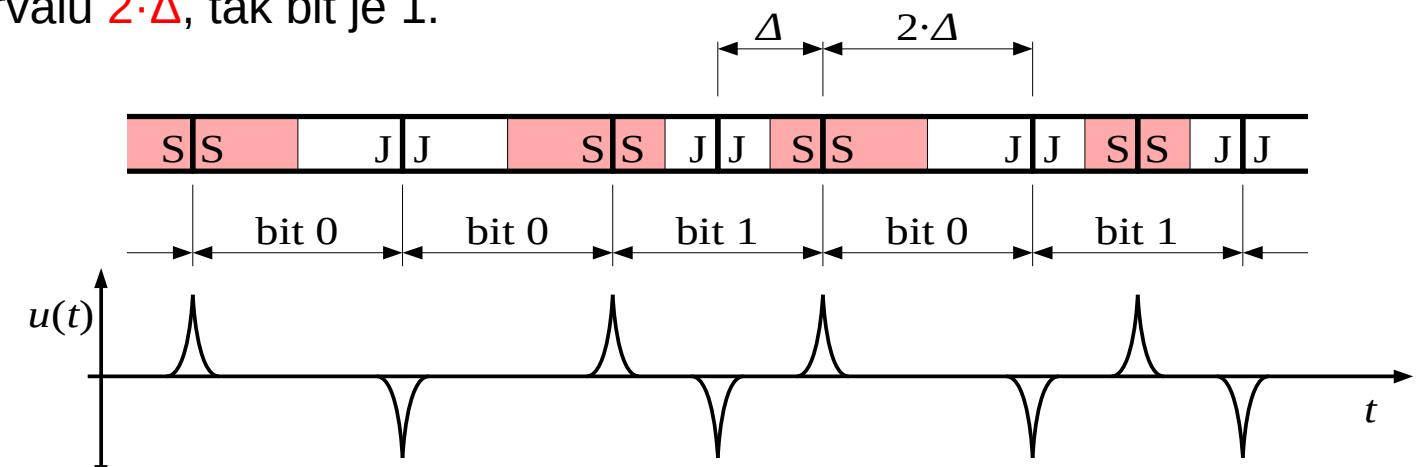
- Autentizační informace se zapisuje na **magnetický pásek** (3 stopy).
- (+) laciné a spolehlivé,
- (-) málo bezpečné (jednoduché klonování).



Stopa	Počet znaků	Počet bitů na znak
1.	79 alfanumerických znaků	7 bitů na znak
2.	40 numerických znaků	5 bitů na znak
3.	107 numerických znaků	5 bitů na znak

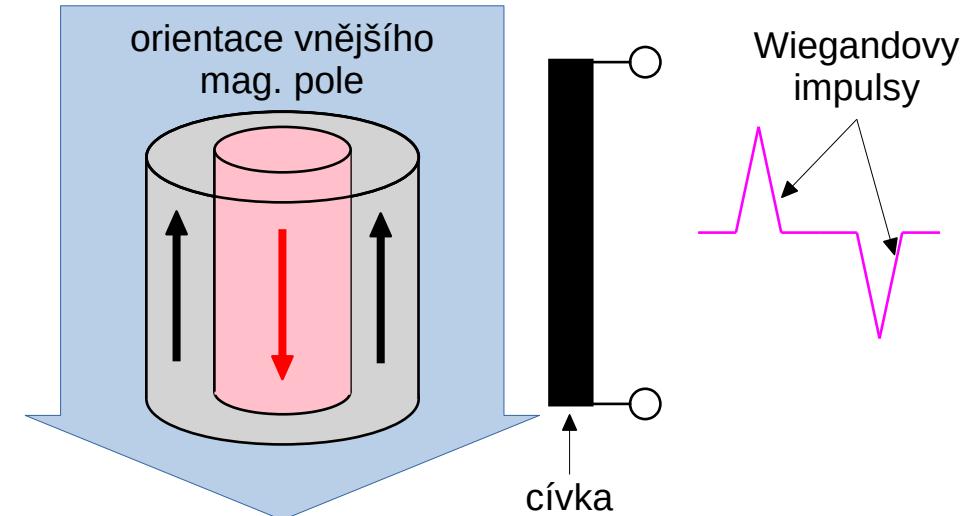
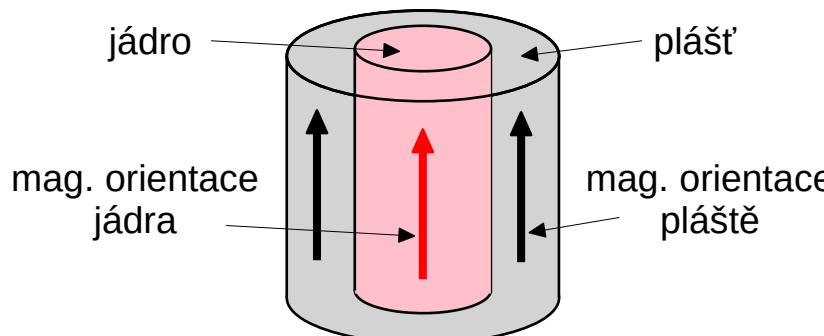
Kódování karty s magnetickým proužkem

- Stopy se magnetizují po **úsecích** o délce Δ a $2 \cdot \Delta$ (viz obrázek). V těchto úsecích je materiál zmagnetizován **jedním** směrem, takže je lze chápat jako ploché permanentní magnety. Na obrázku je orientace těchto magnetů definována pomocí jejich pólů (S = Sever, J = Jih).
- Vždy platí, že **sousedící** magnety též stopy mají **opačné** směry magnetizace, tj. vedle magnetu s orientací S-J je vždy magnet s orientací J-S a naopak.
- Každému **bitu** je ve stopě přidělen úsek o délce $2 \cdot \Delta$, který nazveme bitový úsek. **Nulový** bit se kóduje jako **jediný** magnet o délce Δ a **jedničkový** bit je reprezentován dvojicí **opačně** orientovaných magnetů o délce Δ .
- Magnetický pásek osoba protáhne v blízkosti čtecí hlavy. Na obrázku je časový průběh $u(t)$, který se objeví na **výstupu** této hlavy. Pokud je následující napěťová špička (ta je způsobena rozhraním dvou magnetů) vzdálena úsek $2 \cdot \Delta$, tak jde o bit 0. Pokud se špička nachází uprostřed bitového intervalu $2 \cdot \Delta$, tak bit je 1.



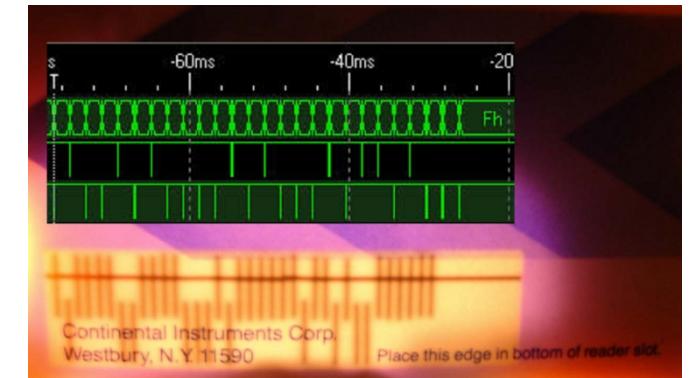
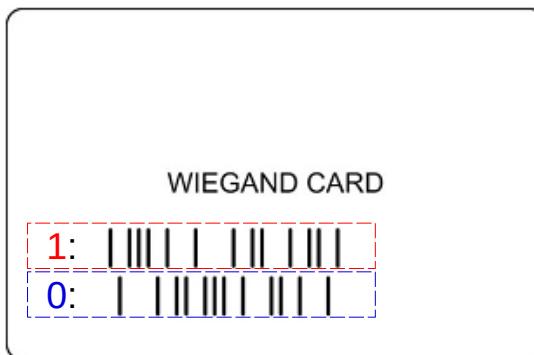
Wiegandův jev

- Wiegandův drát je speciálně zpracovaný drát ze **slitiny** kobaltu, železa a vanadu. Zastudena se za stanoveného tahu opakovaně kroutí a opět vyrovnává.
- Jádro Wiegandova drátu (na obrázku vlevo v růžové barvě) je magneticky **měkké** (tj. lze jej snadno přemagnetovat) a jeho **plášt'** (šedá barva) je magneticky **tvrdý**. Za normální situace jsou orientace magnetického pole jádra (červená šipka) i pláště (černé šipky) stejné.
- V případě výskytu vnějšího magnetického pole, které je **opačné** k magnetické orientaci jádra drátu (na obrázku vpravo modrá šipka), dojde k **přemagnetování** jádra. Tato změna se v blízké cívce projeví velmi krátkou ($\approx 10 \mu\text{s}$) a relativně velkou (až volty) napěťovou **špičkou** (tzv. **Wiegandův jev**). Při **zániku** vnějšího magnetického pole se jádro vlivem působení magnetického pole pláště **vrátí** k původní magnetické orientaci. V cívce tak znikne opačný impuls.



Wiegandova karta

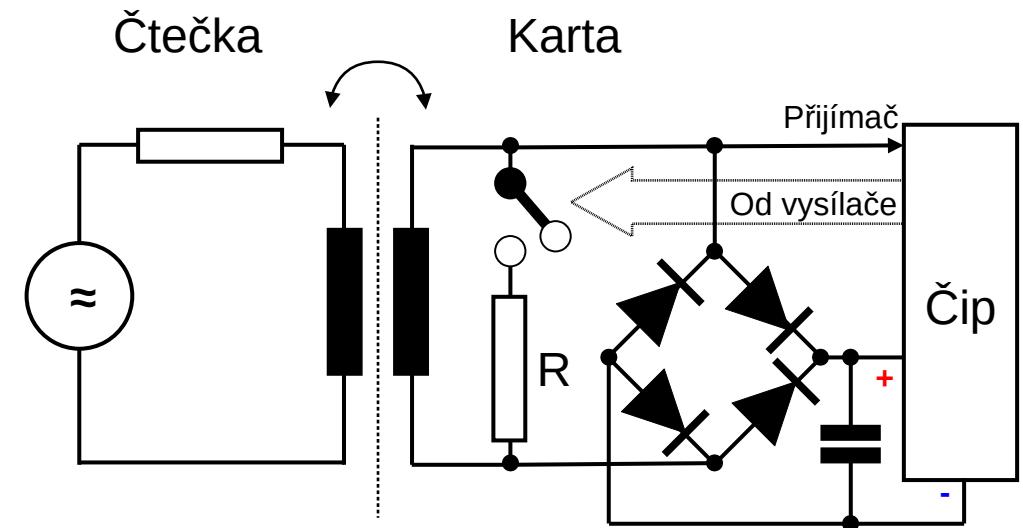
- Do Wiegandovy karty (obrázek vlevo) jsou zalisovány dvě řady 26 Wiegandových drátů. Na každé z 26 pozicí (x-ová souřadnice drátu) se drát nachází buď v horní, nebo v dolní řadě. Horní řada drátů reprezentuje bity o hodnotě 1 a dolní řada bity s hodnotou 0.
 - Ve čtečce (viz obrázek uprostřed) se jak u horní, tak i dolní řady drátů nachází snímací cívka s magnetem, který má opačnou polaritu než zalisované dráty.
 - Pomocí Wiegandova jevu pak lze detektovat, ve které z obou řad se v daném okamžiku nachází Wiegandův drát. Pokud nastane napěťová špička v cívce horní řady, tak se jedná o bit 1 Wiegandova slova a v opačném případě o bit 0 (dva dolní zelené průběhy na obrázku vpravo).
 - Výhodami Wiegandových karet jsou nízká cena, vysoká trvanlivost.
 - Nevýhodou je, že výroba duplikátu je sice obtížnější, ale ne nemožná.



Zapsáno: 10111010010001...

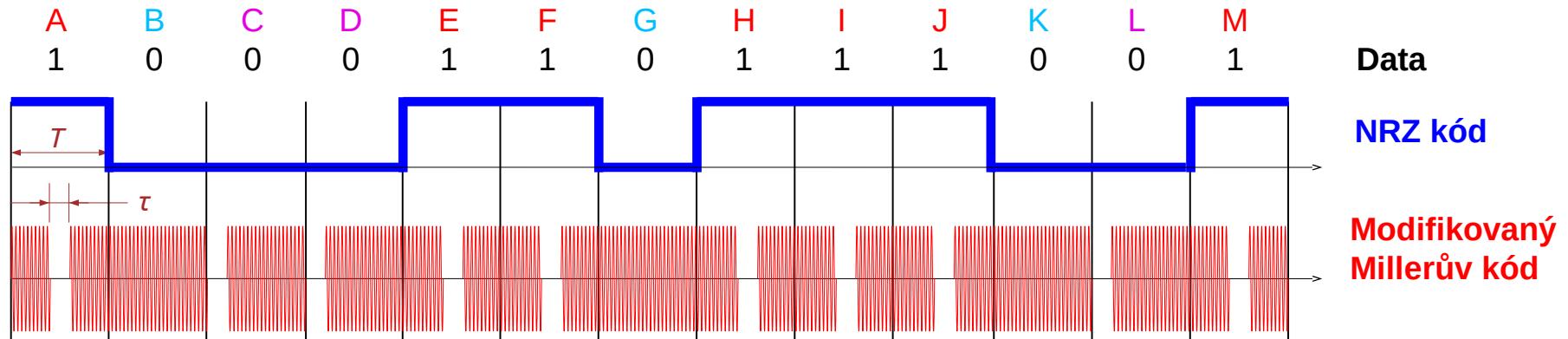
Bezdrátové rozhraní pro karty podle ISO 14443

- Pro bezdrátovou komunikaci mezi čtečkou a kartou RFID, resp. mezi čtečkou a kartou mikroprocesorovou, se používá rozhraní podle standardu **ISO 14443**.
- Karty RFID** („Proximity Card“) fungují se signálem o kmitočtu $f = 125 \text{ kHz}$ a **mikroprocesorové** karty („Smart Card“) pracují se signálem o kmitočtu $f = 13,56 \text{ MHz}$.
- Napájení karty a komunikace je založena na principu **transformátoru**. **Primární** vinutí tohoto transformátoru tvoří cívka čtečky (obr. vlevo) a **sekundární** vinutí tvoří cívka navinutá po obvodu karty (obr. uprostřed).
- Čtečka trvale generuje signál o frekvenci f , který se indukuje v cívce karty (obr. vpravo). Indukované napětí se usměrní a dobíjí se jím **kondenzátor**, který pro čip zalisovaný v kartě (obr. uprostřed dole) funguje jako **zdroj** energie .



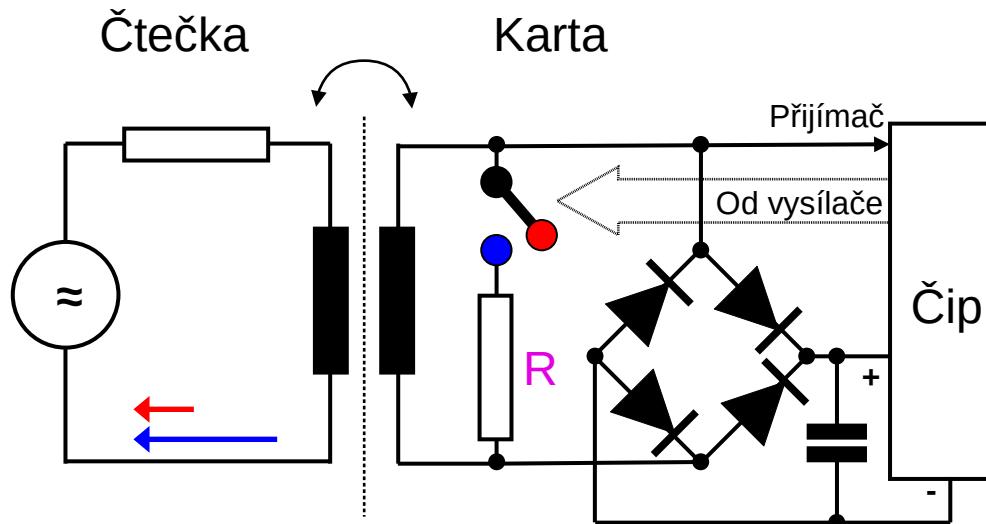
Modifikovaný Millerův kód

- V každém směru komunikace se používá **jiné** kódování.
- Ke komunikaci ve směru **od čtečky ke kartě** se používá modifikovaný **Millerův kód**. Jsou v něm definovány dva stavy - **H** („High“ – čtečka **generuje** nosnou) a **L** („Low“ – čtečka nosnou **negeneruje**). Při zahájení vysílání je první vždy stav H.
- Jednotlivé bity jsou kódovány následovně:
 - "1": v **polovině** délky **T** bitového intervalu se stav H krátkodobě na dobu **τ** změní na stav L (na obrázku to jsou bity **A, E, F, H, I, J** a **M**).
 - "0": pokud je bit "0" za "1", tak se po **celou** dobu **T** generuje stav H (viz bity **B, G** a **K**). V opačném případě se stav H na **začátku** bitového intervalu krátkodobě přeruší na dobu **τ** stavem L (bity **C, D** a **L**).
- Krátkodobý **výpadek** signálu po dobu **τ** je pochopitelně spojen s výpadkem napájení karty. Tento výpadek však karta překlene energií ze svého kondenzátoru.

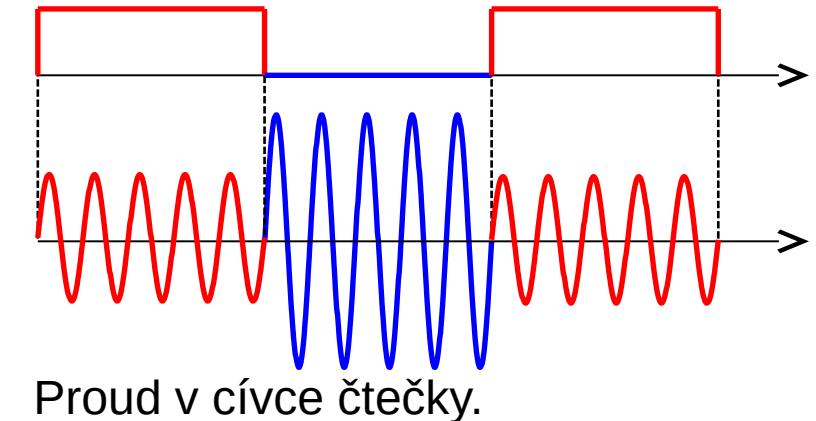


Zátěžová modulace

- Ke komunikaci v opačném směru, ve směru **od karty ke čtečce**, se používá tzv. **zátěžová modulace**. Cívka čtečky funguje jako primární vinutí transformátoru a cívka karty je sekundárním vinutím.
- Čtečka v tomto směru přenosu svojí cívkou **nepřetržitě** generuje harmonický signál o kmitočtu ***f***. Tím je zajištěno napájení karty.
- Data z karty se přenášejí připojováním a odpojováním zátěžového odporu **R** k cívce karty.
- Stav **L** je reprezentován **odpojením** zátěžového odporu **R**. Karta tak odebírá pouze energii k napájení svého čipu, čemuž odpovídá poměrně **malý** proud v cívce čtečky.
- Stav **H** je reprezentován **zapojením** zátěžového odporu **R**. Tím **naroste** proud v cívce karty (sekundáru), což vyvolá nárůst proudu v cívce čtečky (primáru).



Data vysílaná kartou.



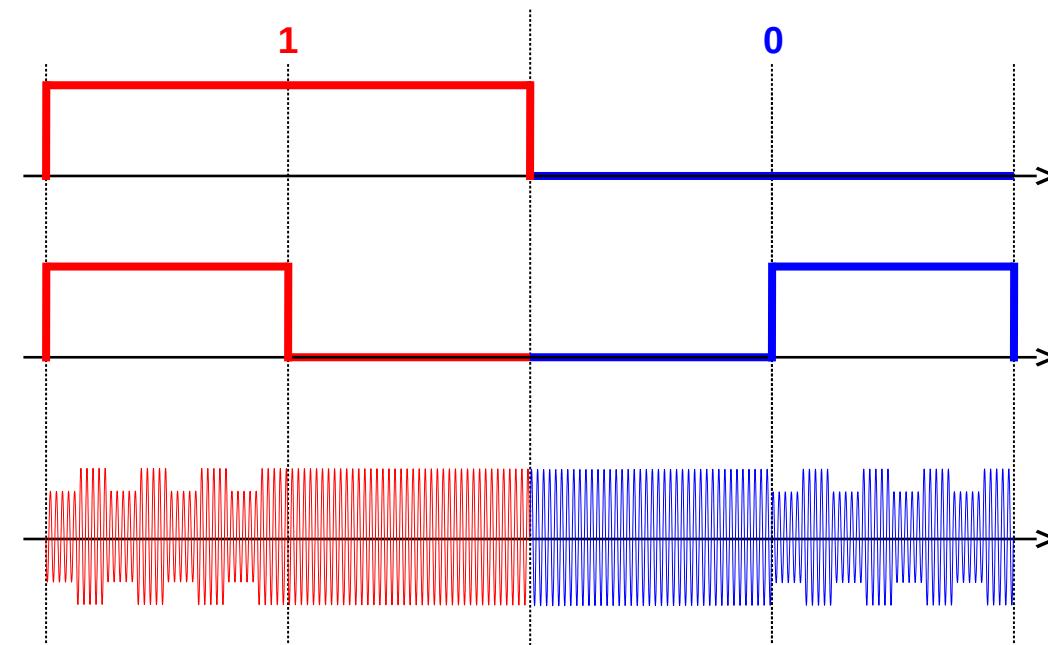
Kódování u zátěžové modulace

- Na obrázku níže je kódování bitů při zátěžové modulaci. Prakticky se jedná o budící signál cívky čtečky o kmitočtu f .
- Bit **1** je reprezentován čtyřmi poklesy úrovně signálu (tj. stavy L) v **první polovině** bitového intervalu.
- Bit **0** je reprezentován čtyřmi poklesy úrovně signálu (tj. stavy L) ve **druhé polovině** bitového intervalu.

Přenášená data

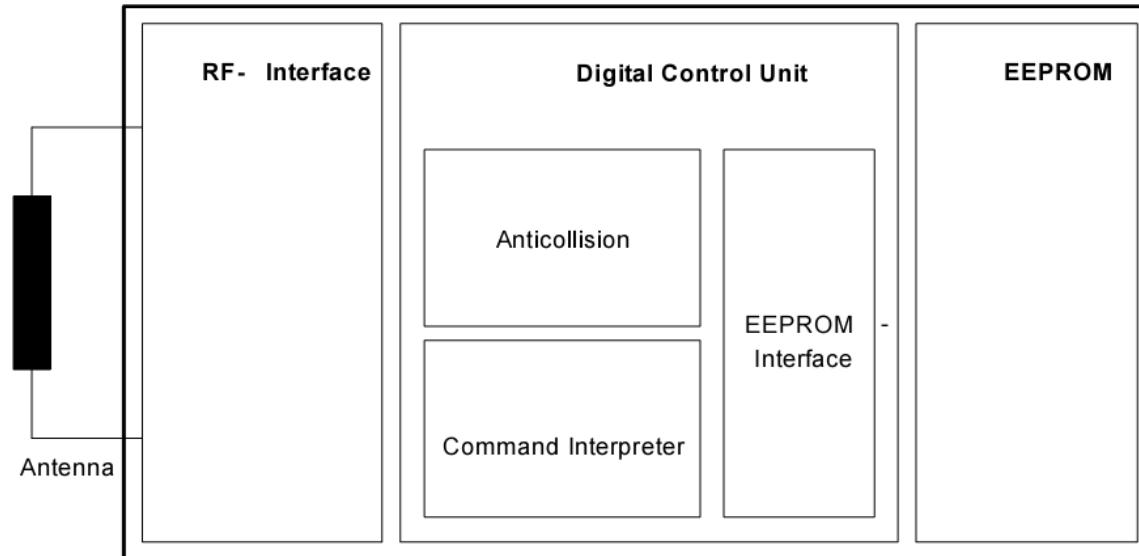
Data v kódu Manchester

Signál zátěžové modulace



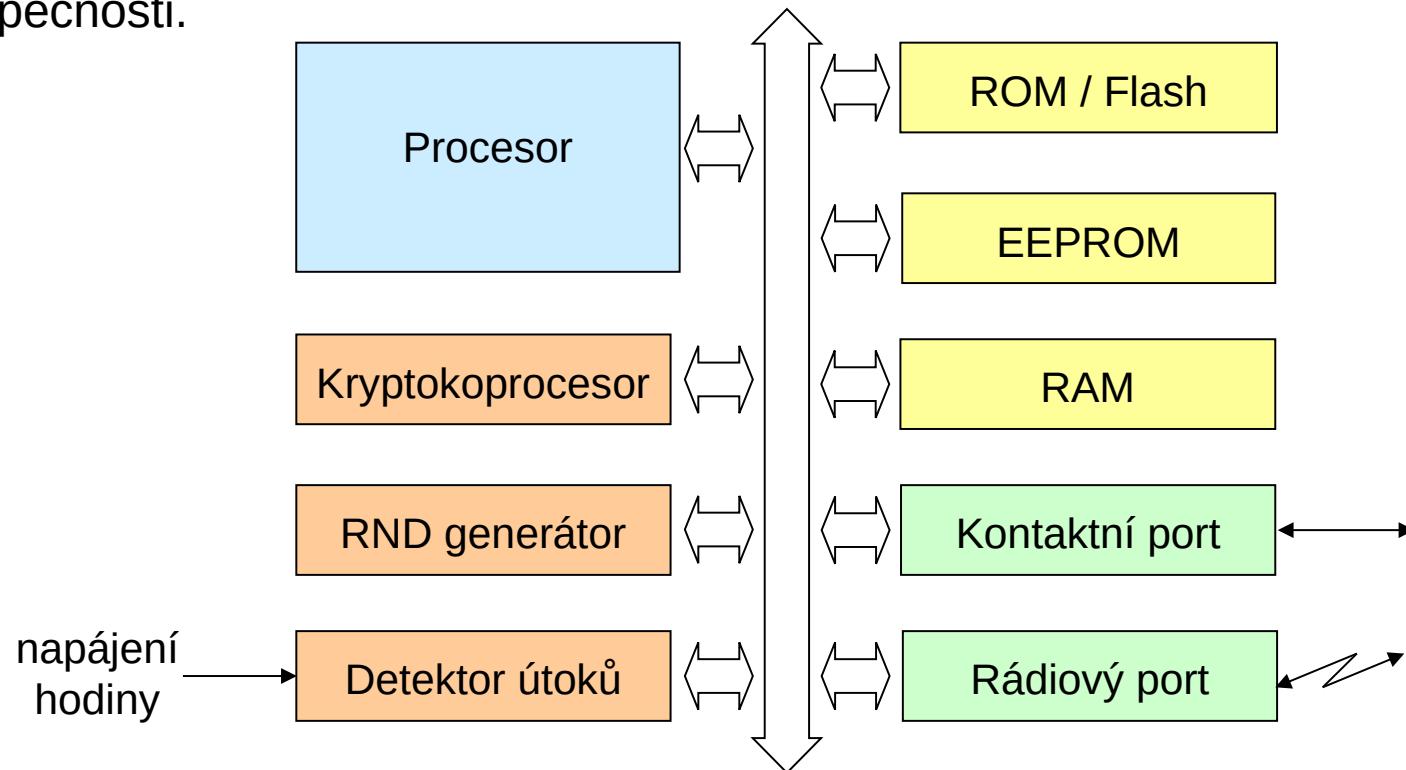
RFID karty

- RFID karty jsou prakticky paměťová úložiště pro **tajné Wiegandovo slovo WS**.
- Zpravidla obsahují **EEPROM** paměť, takže kromě čtení informace umožňují i **zápis** informace.
- Moderní karty poskytují i ochranu před **neoprávněným** čtením tím, že části paměti s Wiegandovým slovem jsou dostupné jen se znalostí tajného hesla na straně čtečky. Karta tak má vlastní přístupový systém.
- Nevýhodou RFID karet je, že **odposlechem** bezdrátové komunikace mezi čtečkou a kartou lze tajnou hodnotu WS zjistit.



Mikroprocesorové karty

- Mikroprocesorové karty jsou prakticky **samostatné** počítače v nichž je dokazovací faktor (klíč symetrického kryptosystému nebo soukromý klíč asymetrického kryptosystému) bezpečně uložen.
- **Kryptoprocesor** zajišťuje náročné kryptografické výpočty jako je například generování dvojice soukromý a veřejný klíč. Soukromý klíč tak nikdy neopustí hranice karty.
- Mikroprocesorové karty se v přístupových systémech používají k zajištění **nejvyšší** bezpečnosti.



Smartfony

- Smartfon (alias chytrý telefon) je prakticky **hybrid** mobilního telefonu a počítače s dotykovým displejem.
- Autentizace smartfonem má tu výhodu, že autentizačním hardwarem je předmět, který vlastní a dennodenně užívá **spousta uživatelů**.
- Výkonnost smartfonů dovoluje nasadit k autentizaci **asymetrickou kryptografií**, která je z provozního hlediska výhodnější. Další výhodou je, že smartfon disponuje **více typy bezdrátových** přenosových technologií, jimiž lze autentizaci provádět.
- Často se používá rozhraní **NFC** („Near field communication“), které je prakticky rozšířením standardu ISO/IEC 14443.
- Výrobci však rovněž nabízejí čtečky s přenosovou technologií **Bluetooth**. Ta již nemá dosah jen řádově centimetry jako NFC, ale má dosah **řádově metry**. Uživatel se tak může autentizovat i několik kroků před vstupem, případně terminál může být umístěn až za překážkou (tj. v kontrolované oblasti), čímž se podstatně snižuje riziko sabotáže terminálu.



5. Závěr

Závěr

- Systémy EKV je elektronický systém určený k **automatizovanému řízení vstupů** v kontrolované oblasti.
- **Docházkové** systémy slouží k **evidenci** přítomnosti osob v prostorách organizace.
- Základními prvky systému EKV jsou **kontrolér, správní jednotka, terminál a vstupy**.
- K autentizaci v systémech EKV se používá znalost **tajných** dat uložených buď v paměti **osoby** (autentizace heslem) nebo v autentizačním **předmětu** (autentizace hardwarem). Další možností je **biometrická** autentizace, které budeme věnovat následující přednášku.
- K autentizaci hardwarem se používají **paměťová** úložiště (karta s magnetickým páskem, Wiegandova karta a RFID karta) nebo **mikropočítače** (mikroprocesorová karta, smartfon).
- Otázka ke zkoušce:

Systémy EKV:

Účel, prvky a architektura systému EKV.

Typy autentizace – princip a vlastnosti.

Karty s magnetickým páskem – princip a vlastnosti.

Bezkontaktní karty podle ISO 14443 – princip a vlastnosti.