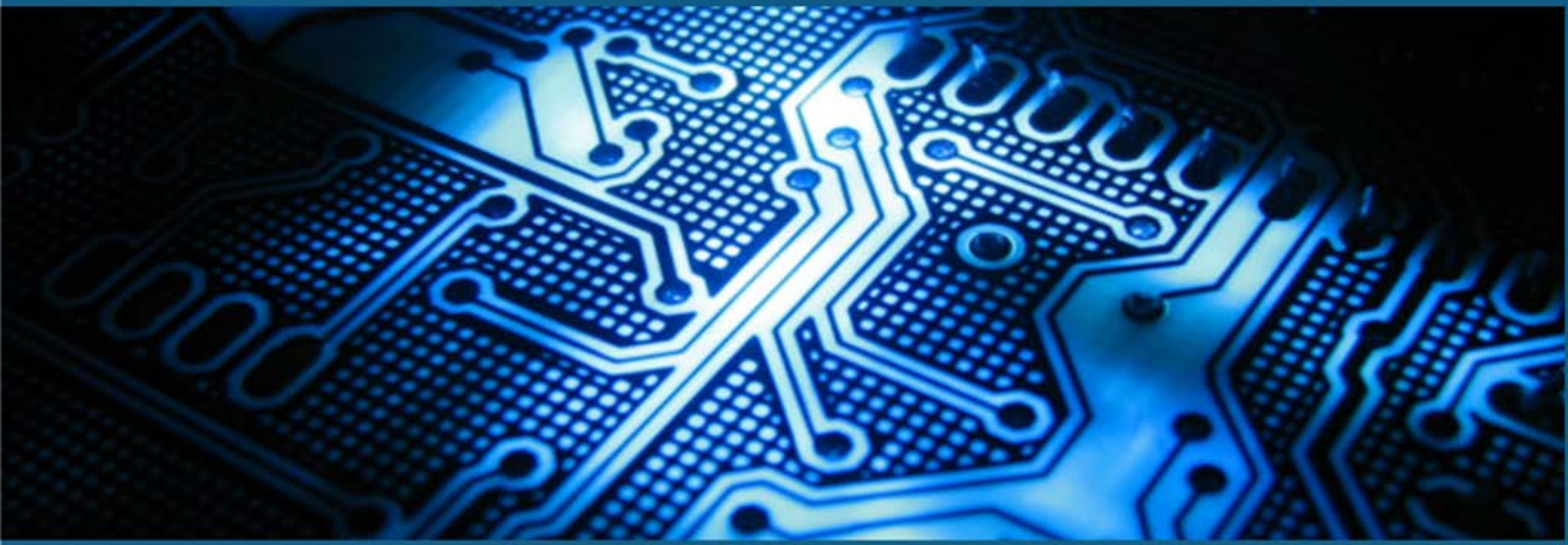
SMART WORLD 2013

share the knowledge



www.konference-smartworld.cz

Rok 2033: Hesla stále s námi?

- DES, 15.1.1977, stáří 36 let (1997 první prolomení)
- Motorola DynaTAC 8000x, 21.9.1983, stáří 30 let
- World Wide Web, 23.8.1991, stáří 22 let
- Smartphones, 16.8.1994, stáří 19 let
- AES, 26.11.2001, stáří 12 let
- Idea NFC, 5.9.2002, stáří 11 let

MONET+

První experimentální web server, Vánoce 1990

Budoucnost v různých barvách...

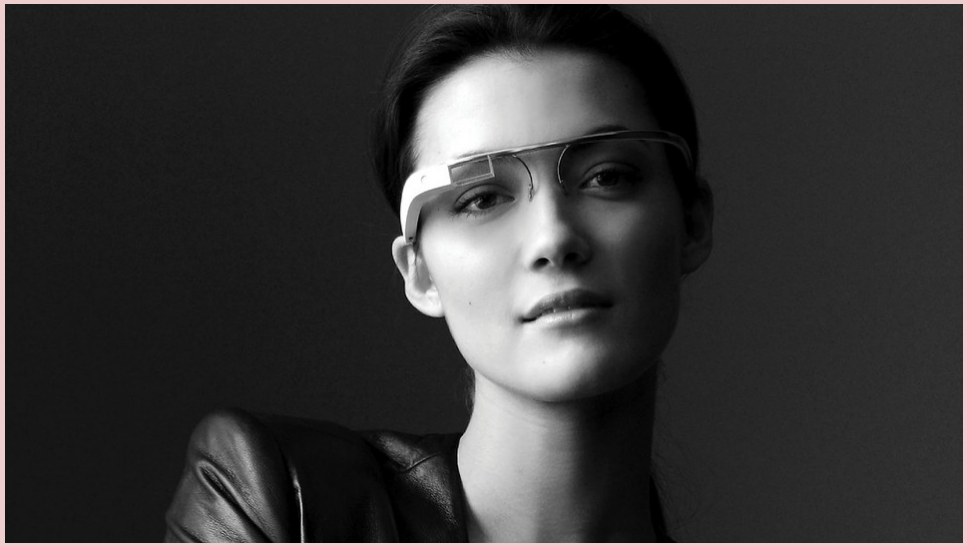
Svět v roce 2033
(Huxleyho Brave New World Rev2)

- Rok 2033 (2 po F.)
  - Rok 1 po F. je první rok po roku, kdy byla vynalezena technologie pro faktorizaci libovolně velkého přirozeného čísla
- Celý (on-line) svět se zhroutil
  - Elektronické zabezpečení komunikací bylo do té doby založeno na RSA algoritmu
  - Od použití ECC algoritmů se upustilo po té, co v rámci aféry PRISM (datována kdysi do druhé poloviny roku 2013) vyšlo najevo, že NSA umí tyto algoritmy prolomit
- Svět se pomalu zotavuje
  - Jsou budovány nové systémy, důvěra v elektronické komunikace bude obnovena až za dalších 12 let (14 po F.)

A co jiný pohled ;)?

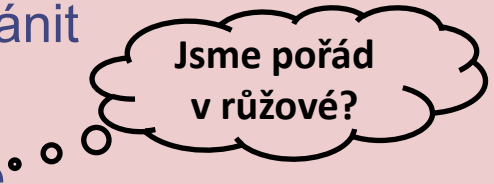
Elektronika se bude víc a víc přibližovat člověku

- Zařízení typu „Google Glass“ a „Smart Wathces“ budou dávno překonaná
- Pro komunikaci bude používán „Brain-computer interface“
- Ale pro představu nám teď stačí ☺



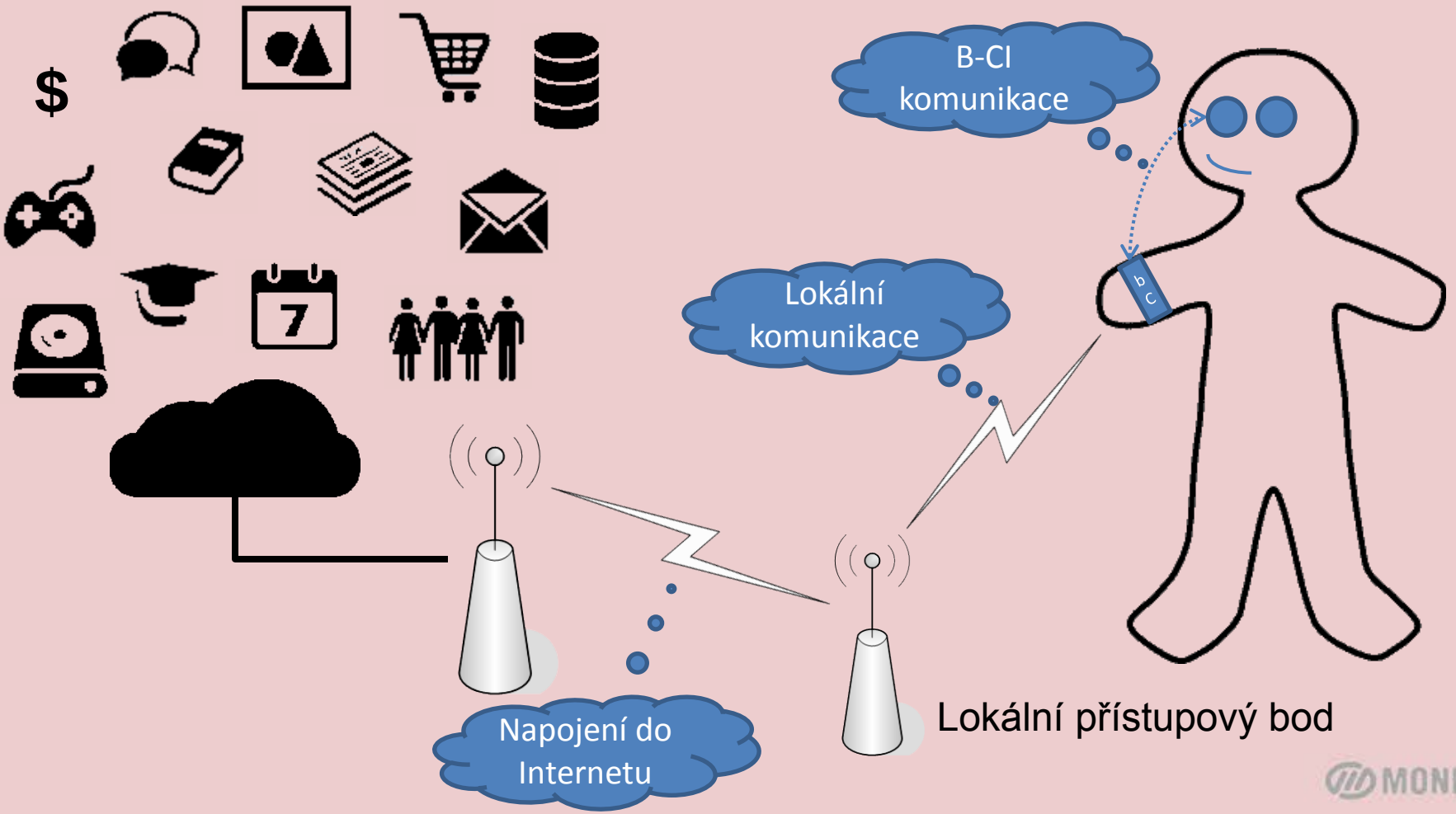
Bezpečnost bude důležitá

- Komunikace a virtuální realita bude tvořit větší a větší část našeho života
- Lidé si budou uvědomovat, že jejich virtuální Já je nutné ve virtuálním světě chránit
- Role státu, regulace

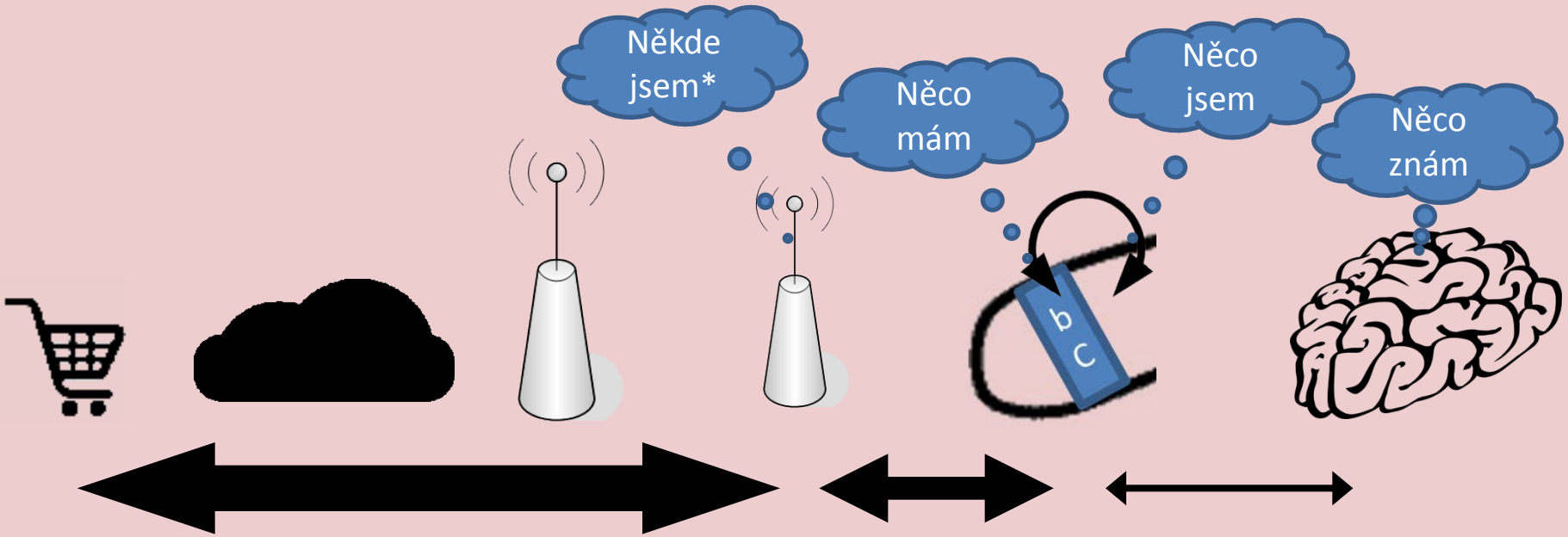


- Systém bude implementovat několika úrovňové zabezpečení
- Zabezpečení nebude klienty obtěžovat

Komunikační řetězec



- V komunikačním řetězci jsou elementy, které se podílejí na zabezpečení
  - Cílem je postupně zvyšovat bezpečnost na cestě od klienta až ke službě



** Čtvrtý faktor „**Někde jsem**“ přidává Vašek Matyáš , snad nám o něm poví víc ☺*

- Ač se to může zdát (ode mě) nečekané, tak i za dvacet let mají hesla růžovou budoucnost
- Bude se zkracovat cesta mezi heslem a zařízení, které jej „přetaví“ na mnohem silnější bezpečnost
  - Dnes např. čipové karty (PIN → kryptografický mechanismus)
- Mohou se měnit formy hesla
  - Podstata zůstane stejná „**Něco znám**“, ale nemusí jít o sekvenci znaků
  - Budou se měnit metody „zadání“ hesla
- S hesly se bude více šetřit
  - Zbývá přece ještě spousta dalších faktorů ;)

Děkuji za pozornost

Milan Hrdlička
milan.hrdlicka@monetplus.cz