Standardy platebních karet a transakcí

Aby mohl globální platební systém fungovat, musí se banky, obchodníci a procesory (např. Shopify) řídit jednotnými technickými normami. Tyto standardy definují vše od fyzického čipu na kartě až po formát zpráv posílaných přes internet.

1. EMV (Europay, Mastercard, Visa)

EMV je globální standard pro čipové karty (Chip-and-PIN) a terminály. Nahradil zastaralé a nebezpečné magnetické proužky.

- **Čip (Integrated Circuit):** Na rozdíl od proužku generuje čip pro každou transakci unikátní kryptografický kód. I když útočník data zachytí, nemůže je znovu použít pro jinou platbu.
- **Tokenizace:** Čip neposílá skutečné číslo karty (PAN), ale jeho zašifrovaný zástupný symbol (token).

—

2. ISO 8583: Jazyk platebních karet

Tento mezinárodní standard definuje formát zpráv, které si mezi sebou vyměňují banky při autorizaci platby.

- **Struktura zprávy:** Obsahuje kód typu zprávy (MTI), bitmapu určující přítomná data a samotné datové prvky (částka, měna, ID terminálu).
- **Proces:** Když zaplatíte v e-shopu, vaše žádost se „zabalí“ do formátu ISO 8583 a putuje k vaší bance ke schválení.

—

3. 3-D Secure (3DS)

Bezpečnostní protokol určený pro platby kartou na internetu (tzv. CNP – Card Not Present).

- **Verze 2.0:** Moderní verze (např. *Verified by Visa* nebo *Mastercard ID Check*), která umožňuje biometrické ověření v mobilní bance (otisk prstu, FaceID).
- **SCA (Strong Customer Authentication):** Požadavek evropské směrnice **PSD2**, který nařizuje dvoufázové ověření u většiny online plateb.

—

4. ISO 20022: Budoucnost plateb

Zatímco ISO 8583 je starší standard pro karty, **ISO 20022** je moderní XML standard pro veškeré finanční zprávy (převody mezi účty, okamžité platby).

- **Bohatá data:** Umožňuje přenášet mnohem více informací o transakci (např. detailní rozpis faktury přímo v platbě).
- **Interoperabilita:** Sjednocuje komunikaci mezi systémy jako SWIFT a vnitrostátními systémy okamžitých plateb.

—

5. Bezpečnostní shoda (Compliance)

Veškeré výše uvedené technologie musí být provozovány v souladu s pravidly pro ochranu dat:

Standard	Zaměření
PCI DSS	Bezpečnostní procesy a infrastruktura.
PCI PTS	Bezpečnost fyzických PIN padů a terminálů.
PCI P2PE	Standard pro šifrování dat od terminálu až k procesorovi (Point-to-Point Encryption).

Související články:

- PCI DSS: Technické požadavky
- Kryptografie: Základ bezpečných plateb
- Architektura finančních systémů

Tagy: it finance standards pci-dss emv iso8583 3ds cybersecurity