E-Banking Authentication

Dynamic Password Generators and Hardware Tokens

Author: Ondřej Hujňák

30.5.2022

IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received January 10, 2022, accepted January 21, 2022, date of publication February 7, 2022, date of current version February 15, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3149475

E-Banking Security Study—10 Years Later

KAMIL MALINKA, ONDŘEJ HUJŇÁK, PETR HANÁČEK, AND LUKÁŠ HELLEBRANDT
Faculty of Information Technology, Brno University of Technology, 612 00 Brno, Czech Republic

Corresponding author: Kamil Malinka (malinka@fit.vutbr.cz)

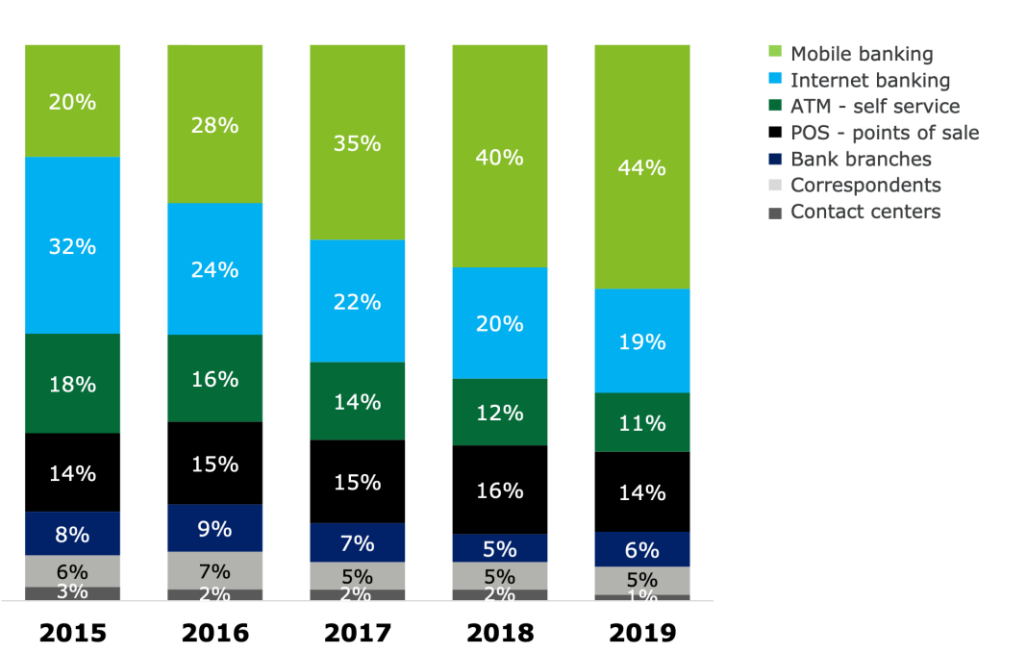
This work was supported by the Internal Project of Brno University of Technology (BUT) under Grant IGA FIT-S-20-6427.

ABSTRACT ICT security in the banki [illegible] is going th [illegible] gh rapid changes. It is ten years since we covered the state of e-banking security, [illegible] lation has evolved. With the Payment Services Directive (PSD2) [illegible] believe it is a good time to update our findings. PSD2 brings new [illegible] tion, thus it is necessary to revise compliance of currently used sc [illegible] is an overview of current authentication methods, their properties w [illegible] d their resistance against attacks. We further discuss the multi-fac [illegible] of those methods and their compliance with the PSD2 requirement [illegible] introduced the e-banking attacks taxonomy, which is compatible w [illegible] al Identity Guidelines but has an increased level of detail with re [illegible] sources in this area are usually either very broad, targeted on th [illegible] articular issue or attack in greater detail. We believe our article ca [illegible] a comprehensive and complex tool to help with orientation in [illegible]

INDEX TERMS Online banking, PSD2, authentication, multi-factor, cybersecurity, secure hardware.

Motivace

- Posun od internetového k mobilnímu bankovnictví



Banking transactions *FEBRABAN, Brazílie*

- Nové možnosti a způsoby autentizace
- Nová legislativa – Revised Payment Service Directive (PSD2)

Obsah

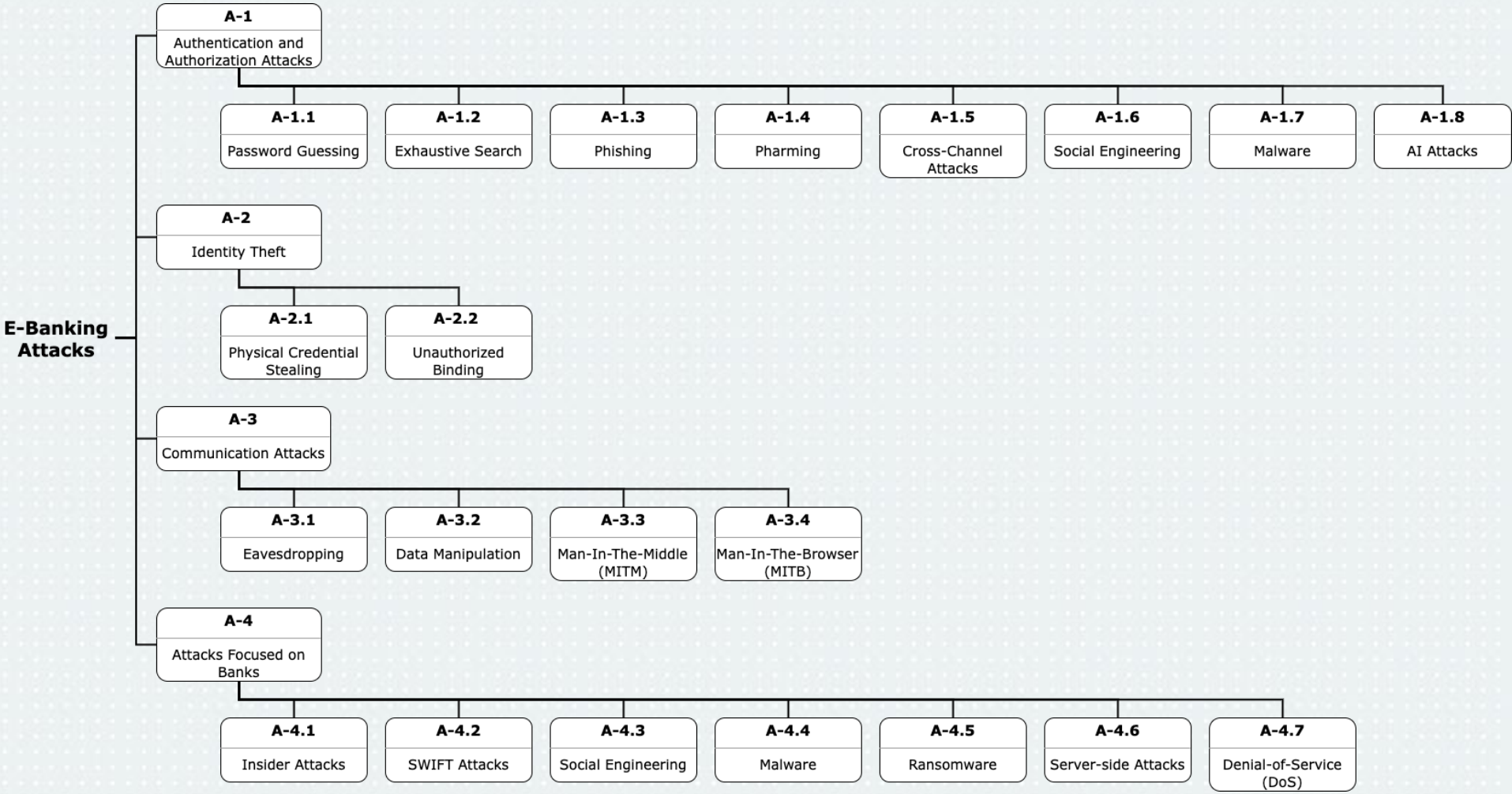
- Útoky na elektronické bankovnictví
- Revised Payment Service Directive (PSD2)
- Autentizační primitiva
  - Dynamic password generators (DPG)
  - Hardware security module (HSM) and enclave
- Autentizační metody a schémata
  - Trendy
- Fast Identity Online (FIDO)

Útoky na elektronické bankovnictví

- Referenční taxonomie útoků
  - NIST Digital Identity Guidelines

- Čtyři hlavní skupiny útoků
  - Útoky na autentizaci a autorizaci
  - Krádež identity
  - Útoky na komunikaci
  - Útoky na bankovní systémy

Taxonomie útoků



Revised Payment Service Directive

- Nařízení EU upravující platební služby na evropském trhu.
- V platnosti od 14. září 2019 (SCA povinné od 31. prosince 2020)
- Cíle:
  - Zvýšení ochrany spotřebitele (definování „strong customer authentication“)
  - Zlepšení hospodářské soutěže (přístup třetích stran – API, multibanking)
  - Stimulovat inovace
  - Definovat práva a povinnosti poskytovatelů plateb a služeb

DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2015

on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Commission Delegated Regulation (EU) 2018/389

- Kromě PSD2 existuje i prováděcí regulace
- Specifikuje technické detaily
  - Požadavky na auditovatelnost
  - Požadavky na kvalitu rozhraní
  - Technologickou neutralitu při implementaci autentizačních kódů
  - Použití **otevřených standardů**
  - Definuje výjimky pro SCA
    - Většinou na základě typu transakce a správy rizik

Klientská autentizace dle PSD2

- **Silné ověření klienta (SCA)**
  - Povinnost minimálně dvou-faktorové autentizace
  - Vynucena nezávislost faktorů
- **Dynamické propojení**
  - Svázání autentizačního kódu s konkrétní transakcí
- U faktoru držení či vlastnictví (possession) vynucena ochrana proti klonování

  „*The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.*”

Silné ověření klienta

*„strong customer authentication" means an authentication based on the use of **two or more elements** categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are **independent**, in that the **breach of one does not compromise** the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.*

Nezávislost faktorů

1. *Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.*

2. *Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.*

3. *For the purposes of paragraph 2, the mitigating measures shall include each of the following:*

   a) *the use of separated secure execution environments through the software installed inside the multi-purpose device;*
   b) *mechanisms to ensure that the software or device has not been altered by the payer or by a third party;*
   c) *where alterations have taken place, mechanisms to mitigate the consequences thereof.*

Dynamické propojení

1. *Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:*

   a) *the payer is made aware of the amount of the payment transaction and of the payee;*
   b) *the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;*
   c) *the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;*
   d) *any change to the amount or the payee results in the invalidation of the authentication code generated.*

Autentizační primitiva

	Primitive	Replay Resistance	MITM Resistance	Impersonation Resistance
P-MSC	Memorized secret	✗	✗	✗
P-LUS	Look-up secret	✓	✗	✗
P-SCR	Single-factor cryptographic authentication	✓	✓	✓
P-MCR	Multi-factor cryptographic authentication	✓	✓	✓
P-MFO	Multi-factor OTP device	✓	✓	✓
P-OOB	Out-of-band authentication	✓	✗	✗
P-SFO	Single-factor OTP device	✓	✓	✓
P-BIO	Biometric authentication	✗	✗	✗

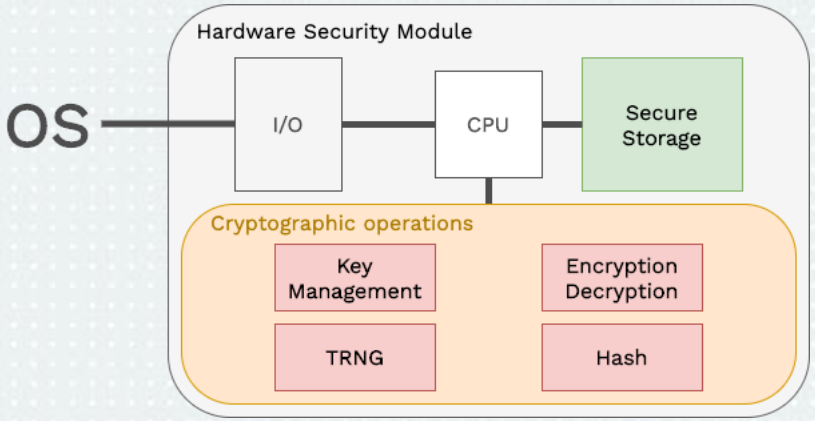
- Odolnost proti zosobnění – ověřitelná identita a nepopiratelnost

Dynamic password generator

- Simulace HW tokenů v SW (generátor OTP)
- Moderním trendem jsou DPG ve formě mobilních aplikací
  - Často challenge – response
- Integrované DPG
  - součástí mobilního bankovnictví (P-SFO)
  - Splňuje SCA pokud využívá HSM/enklávu, jinak je nedořešeno
- Separátní DPG
  - samostatná aplikace (P-MFO→ OTP + possession)
  - Pokud považujeme izolaci aplikací v mobilních OS za bezpečnou, můžeme považovat za nezávislý faktor i bez HSM/enklávy

Hardware security module

- Speciální modul poskytující kryptografické operace
- Hardware navržen pro odolnost proti fyzickým útokům
- Vlastnosti HSM umožňují:
  - Uložení dat, která mají omezen způsob manipulace (čítač)
  - Izolaci kryptografických operací a klíčů
  - Kontrolu integrity systému (atestaci)

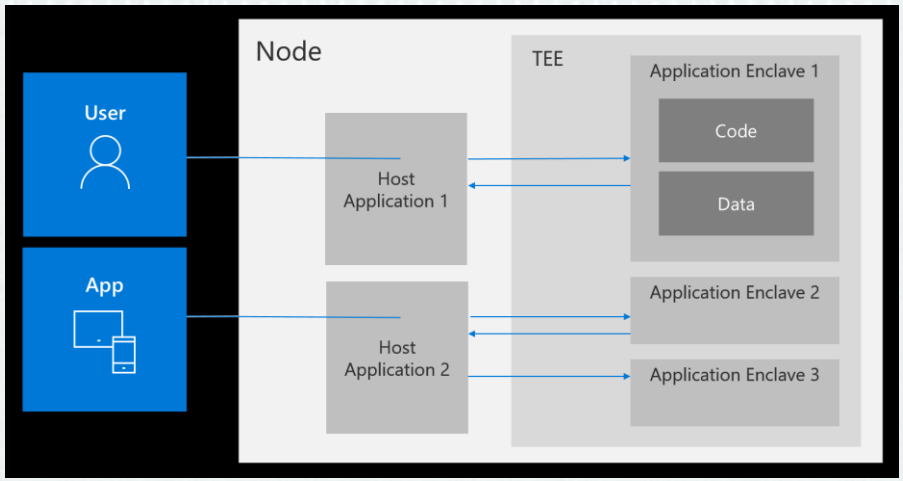


Hardware security module

- Možnosti zapojení HSM:
  - Samostatný čip, který je umístěn na základové desce (Trusted Platform Module, smartphone)
  - Dedikovaný HW připojený nějakým rozhraním (PCI, ethernet, USB, NFC, Bluetooth)
- Rozšířením funkčnosti HSM jsou enklávy

Enkláva

- Implementuje Trusted Execution Environment (TEE)
  - Izolace běžící aplikace od OS
  - Zajištění důvěrnosti, integrity a bezpečí běžící aplikace před vnějšími hrozbami
- Na rozdíl od HSM umožňuje běh vlastních aplikací
- Příklady enkláv: Intel SGX, ARM TrustZone



Open Enclave SDK

Bezpečný hardware u smartphone

- Podpora HSM a enkláv je i v moderních mobilních telefonech
- **Apple Secure Enclave (ASE)**
  - Již od iPhone 5
  - Úzce integrována se systémem (Touch ID, Face ID)
- **Android Keystore System (AKS)**
  - Zastřešuje přístup, ale není vázáno na konkrétní bezpečnostní modul
  - Na základě typu přítomného modulu poskytuje:
    - Secure Element – pouze bezpečné úložiště klíčů
    - HSM – plnohodnotný HSM chip podporující i kryptografické operace
    - TEE – obsahuje enklávu umožňující bezpečný běh aplikací

Autentizační metody

	Password Guessing A-1.1	Exhaustive Search A-1.2	Social engineering (Phishing) A-1.3, A-1.6	Pharming A-1.4	Cross-channel attacks A-1.5	Malware A-1.7	AI Attacks A-1.8	Physical credential stealing A-2.1	Unauthorised Binding A-2.2	Eavesdropping A-3.1	Data manipulation A-3.2	MITM A-3.3, A-3.4
Static password, PIN (P-MSC)	✓	✓	✓	✓	N/A	✓	✗	✗	(✓)[1]	(✓)[2]	✓	✓
Grid card (P-LUS)	✗	✓	✓	✓	N/A	✗	✗	✓	(✓)[1]	✗	✓	✓
Dynamic password generator (P-SFO)	✗	✗	✗	(✗)[3]	(✓)[4]	✓	✗	✓	✓	✗	(✗)[3]	(✗)[3]
PKI (P-SCR)	✗	✗	✗	✗	N/A	✓	✗	✗	✓	✗	✗	✗
PKI token (P-MCR)	✗	✗	✗	✗	N/A	✓	✗	✓	✓	✗	✗	✗
SMS Code (P-OOB)	✗	(✓)[5]	✗	✓	✓	✓	✗	✓	✓	✓	(✗)[3]	(✗)[3]
HW tokens with display (P-MFO)	✗	(✓)[5]	✗	(✗)[3]	N/A	✗	✗	✓	✓	✗	(✗)[3]	(✗)[3]
HW tokens without display (P-MFO)	✗	(✓)[5]	✗	✓	N/A	✓	✗	✓	✓	✗	(✗)[3]	(✗)[3]
Secure Enclave (P-MFO)	(✓)[6]	✓	✗	✗	N/A	✓	✗	✓	✓	✗	✗	✗
Biometric authentication (P-BIO)	✗	✗	✗	✓	N/A	✓	✓	✗	✓	(✓)[7]	✓	✓

[1] In case the user can reset the authentication method (password reset, resend grid card) the attack is possible.
[2] If there is no HSTS header set, an adversary might force unencrypted connection.
[3] The method is vulnerable in case that it does not support Dynamic Linking as defined in PSD2 directive.
[4] Applies only if the DPG is running on different device than e-banking (2da – see section IV-B).
[5] In case the length of the one-time cryptogram is not sufficient, and attempts are not limited.
[6] If the enclave is unlocked by a password, an attacker may use password guessing.
[7] Depends on the implementation parameters.

Autentizační schémata

Method combination	Cloning protection	Factor independence	Dynamic linking	SCA	Comment
SMS	(✓)[2]	✗	Opt.	✗	oob
Password + SMS	(✓)[2]	✓	Opt.	(✓)[3]	oob
Integrated DPG protected by password (SFO)	(✗)[4]	(✗)[5]	✓	(✗)[5]	1aa
Separated DPG protected by password (MFO)	(✗)[4]	(✓)[4]	✓	(✓)[4]	2aa
Dynamic password + BIO	(✗)[4]	✓	✓	(✓)[4]	2aa
BIO + Password	✗	✓	✗	✓	
BIO + SMS	(✓)[2]	✓	Opt.	✓	oob

•••

[2] Indirectly possible by attacks on telecommunication links such as SIM Swapping and SS7 attacks.
[3] To fulfil SCA requirements, the SMS receiving device have to be independent of the other one where the password is entered. Nowadays, this is difficult to achieve.
[4] Depends on OS capabilities, in case of rooted OS (called jailbreak in iOS) cannot be ensured [78]. E.g. biometrics is cloneable by design, and protection depends on second factor properties.
[5] The satisfiability of factor independence is not decided yet; if it does not satisfy factor independence, it isn't SCA.

Autentizační schémata

Method combination	Cloning protection	Factor independence	Dynamic linking	SCA	Comment
PKI (private key) protected by password	✓	✗	✓	✗	
HW Token (MCR)	✓	✓	✓	✓	2da
HW Token protected by PIN	✓	✓	✓	✓	2da
HW Token protected by BIO	✓	✓	✓	✓	2da
PKI (private key) protected by BIO	(✗)[4]	✗	✓	✗	
Secure Enclave protected by BIO	✓	✓	✓	✓	
Secure Enclave protected by password	✓	✓	✓	✓	

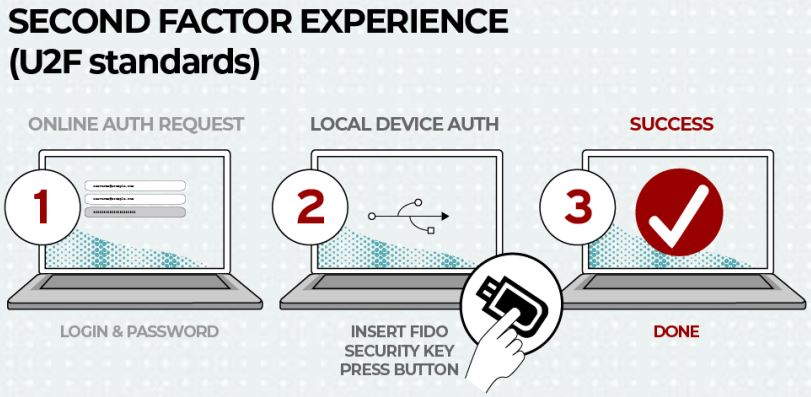
[4] Depends on OS capabilities, in case of rooted OS (called jailbreak in iOS) cannot be ensured [78]. E.g. biometrics is cloneable by design, and protection depends on second factor properties.

Trendy v autentizaci

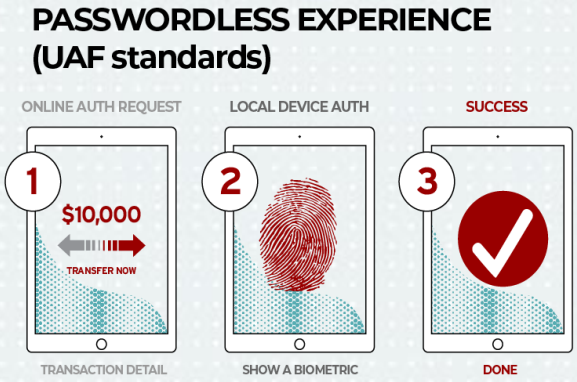
- **Biometrika**
  - Převládá v autentizaci na smartphonech (ale může být i u HW tokenů…)
  - Používá se v KYC procesu pro vzdálené ověření uživatele
- **Enkláva**
  - Relativně nový bezpečnostní prvek
  - Většinou chráněn dalším faktorem (heslo, PIN, biometrika)
- **Dynamic Password Generator**
  - E-banking systémy v EU kvůli PSD2
- **FIDO2**
  - Současný otevřený standard pro HW tokeny a biometriku
  - Zatím spíše FinTech, z bank Bank of America a Boursorama Banque

Fast Identity Online

- Universal 2nd Factor (U2F)
  - Vydán 2014
  - Google + Yubico
  - Proprietární standard pro silnou autentizaci pomocí HW tokenu

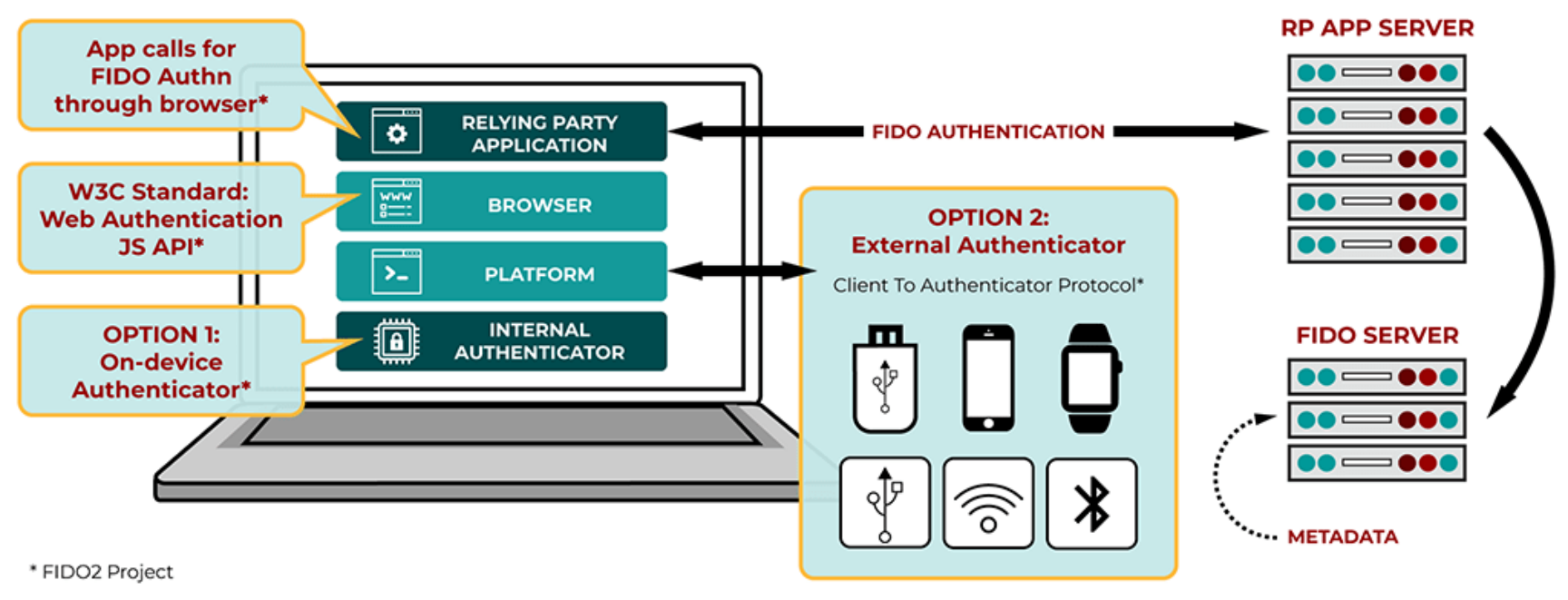


- Universal Authentication Factor (UAF)
  - Vydán 2014
  - Framework pro nahrazení autentizace heslem lokálním ověřením (primárně biometrie)



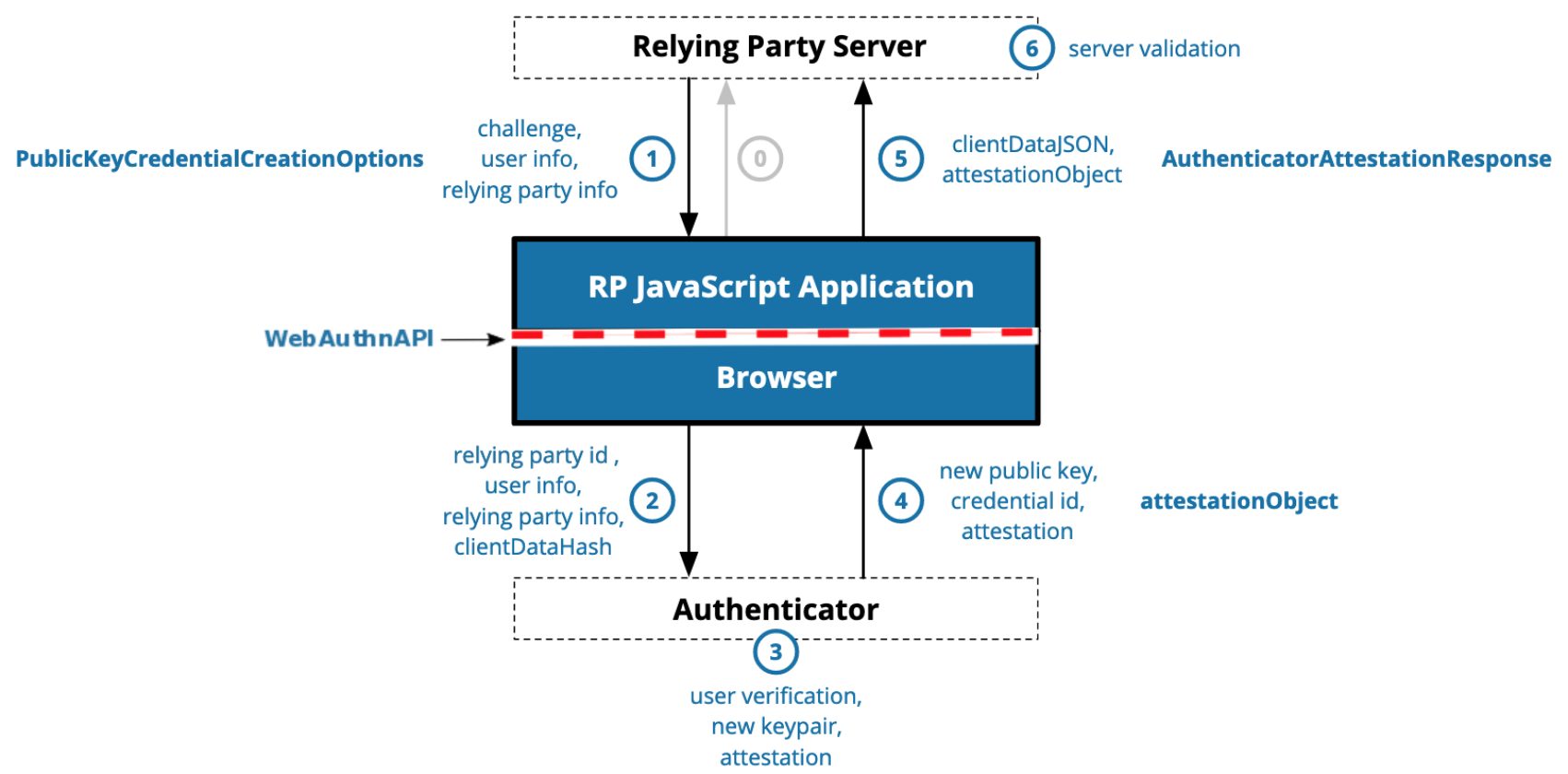
FIDO2

- Otevřený standard pro autentizaci
  - W3C WebAuthn
  - CTAP



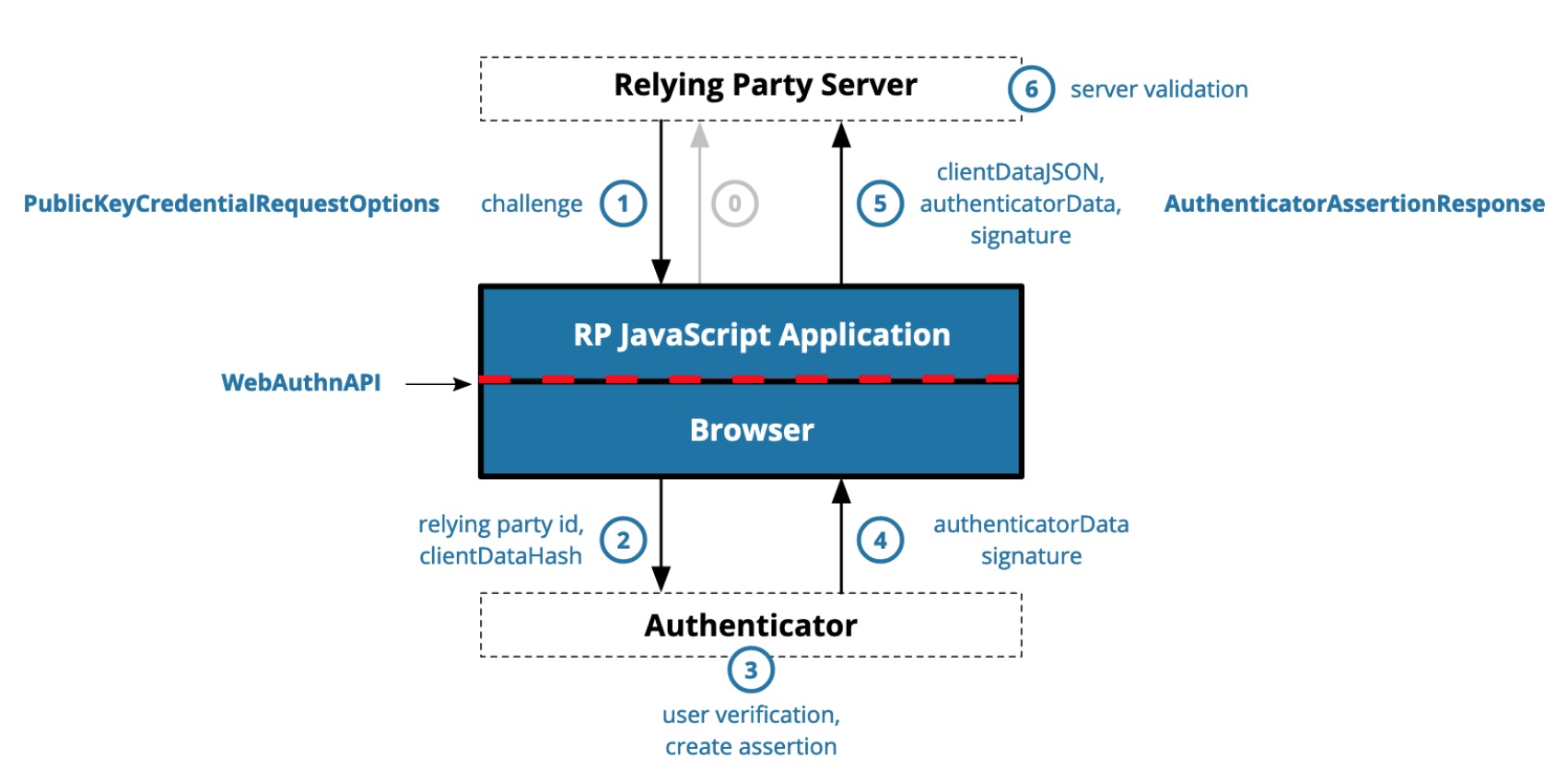
FIDO2 – Registrace

```
const assertion = await navigator.credentials.create(options)
```



FIDO2 – Autentizace

```
const assertion = await navigator.credentials.get(options)
```

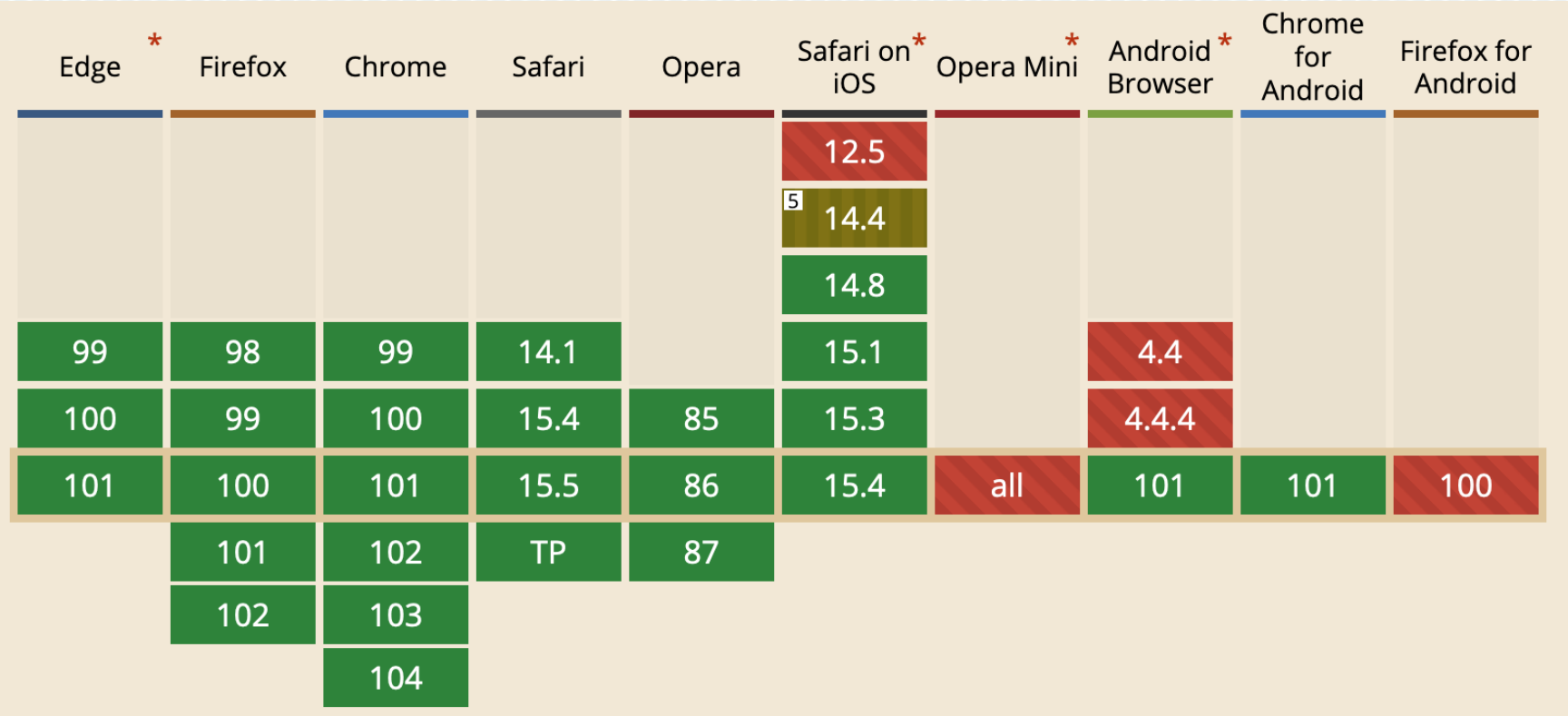


Client To Authenticator Protocol

- Komplementární protokol k WebAuthn
- FIDO U2F: CTAP1/U2F
- FIDO2: CTAP2
  - Autentikátor implementující CTAP2 označován jako FIDO2 autentikátor
- Slouží k připojení externích autentikátorů

  či uživatelských kryptografických autentikátorů (HSM)

FIDO2 – Podpora v prohlížečích



Edge *	Firefox	Chrome	Safari	Opera	Safari on iOS *	Opera Mini *	Android Browser *	Chrome for Android	Firefox for Android
					12.5				
					5 14.4				
					14.8				
99	98	99	14.1		15.1		4.4		
100	99	100	15.4	85	15.3		4.4.4		
101	100	101	15.5	86	15.4	all	101	101	100
	101	102	TP	87					
	102	103							
		104							

Podpora FIDO v bankovnictví

- Banky světově:
  - Bank of America – člen FIDO Alliance, podporuje FIDO2
  - Boursorama Banque – podpora FIDO2
  - ING Bank – podpora FIDO UAF v rámci *Xtrong Authentication Suite*
- Banky u nás:

Podpora FIDO mimo bankovnictví

- Velké množství webových služeb, zahrnují i FinTech
  https://fidoalliance.org/certification/fido-certified-products/
- V **ČR** podpora **MojeID** pro přístup ke službám státní správy
  - Pro některé operce vyžaduje přístup k autentikátoru chráněný PINem
- Podpora pro přihlašování do OS
  - Windows Hello
  - Linux PAM
  - MacOS login
- Podpora v nástrojích pro šifrování disku
  - LUKS

Diskuse