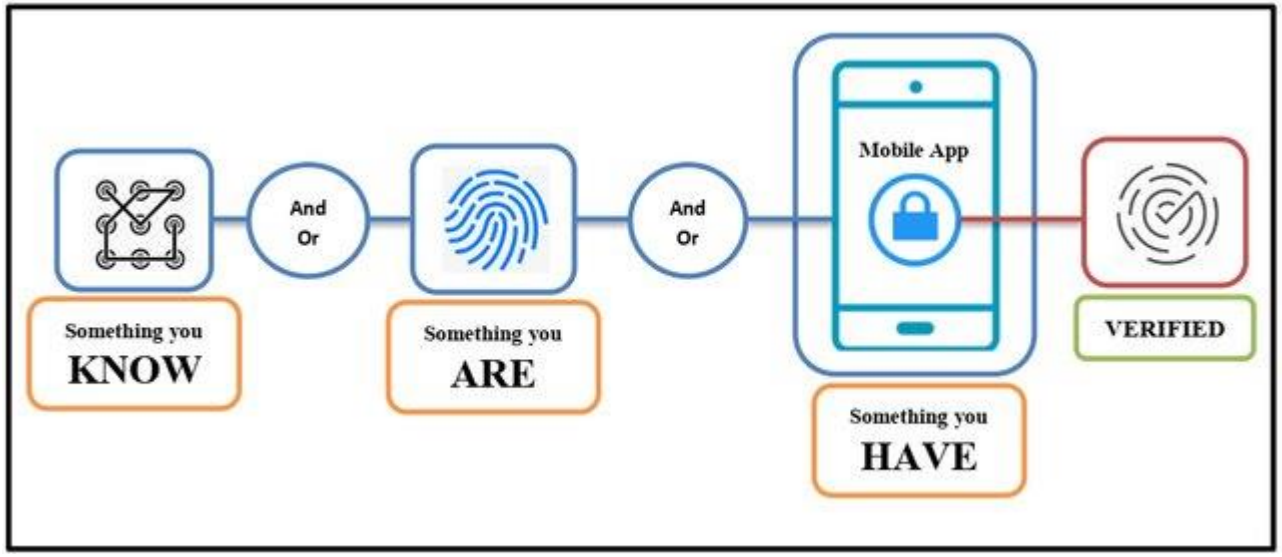
Autentificarea Multi-factor. Procesul de *challenge-response.* Phishing

Conf. Univ. Dr. Marius Iulian Mihăilescu
m.mihailescu.mi@spiruharet.ro
https://www.mariusmihailescu.com

30.09.2022

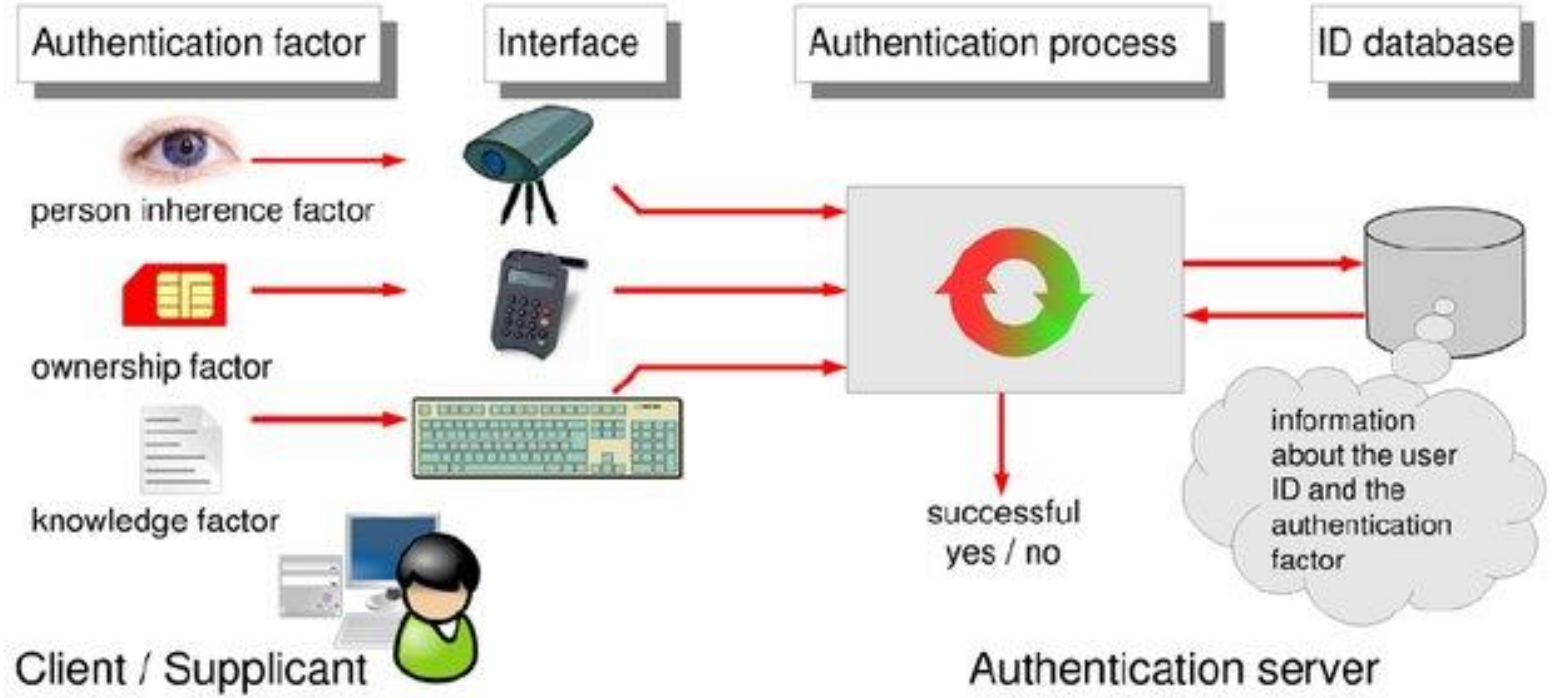
Autentificarea multi-factor

- Autentificarea multi-factor reprezintă o metodă de autentificare electronică în care utilizatorul primește acces la o aplicație web sau software doar după ce a reușit să prezinte două sau mai multe componente (factori) de evidență unui mecanism de autentificare.
- Factorii sunt clasificați astfel:
  - Ceva ce UTILIZATORUL CUNOAȘTE – parole, pin etc.
  - Ceva ce UTILIZATORUL ARE - orice obiect fizic aflat în posesia utilizatorului, precum un token (USB stick), card bancar, cheie etc.
  - Ceva ce UTILIZATORUL ESTE – caracteristici fizice (biometrice – vezi prelegerea anterioară), precum amprenta digitală, iris, viteza de tastatare, pattern-uri în comportamentul de tastare..



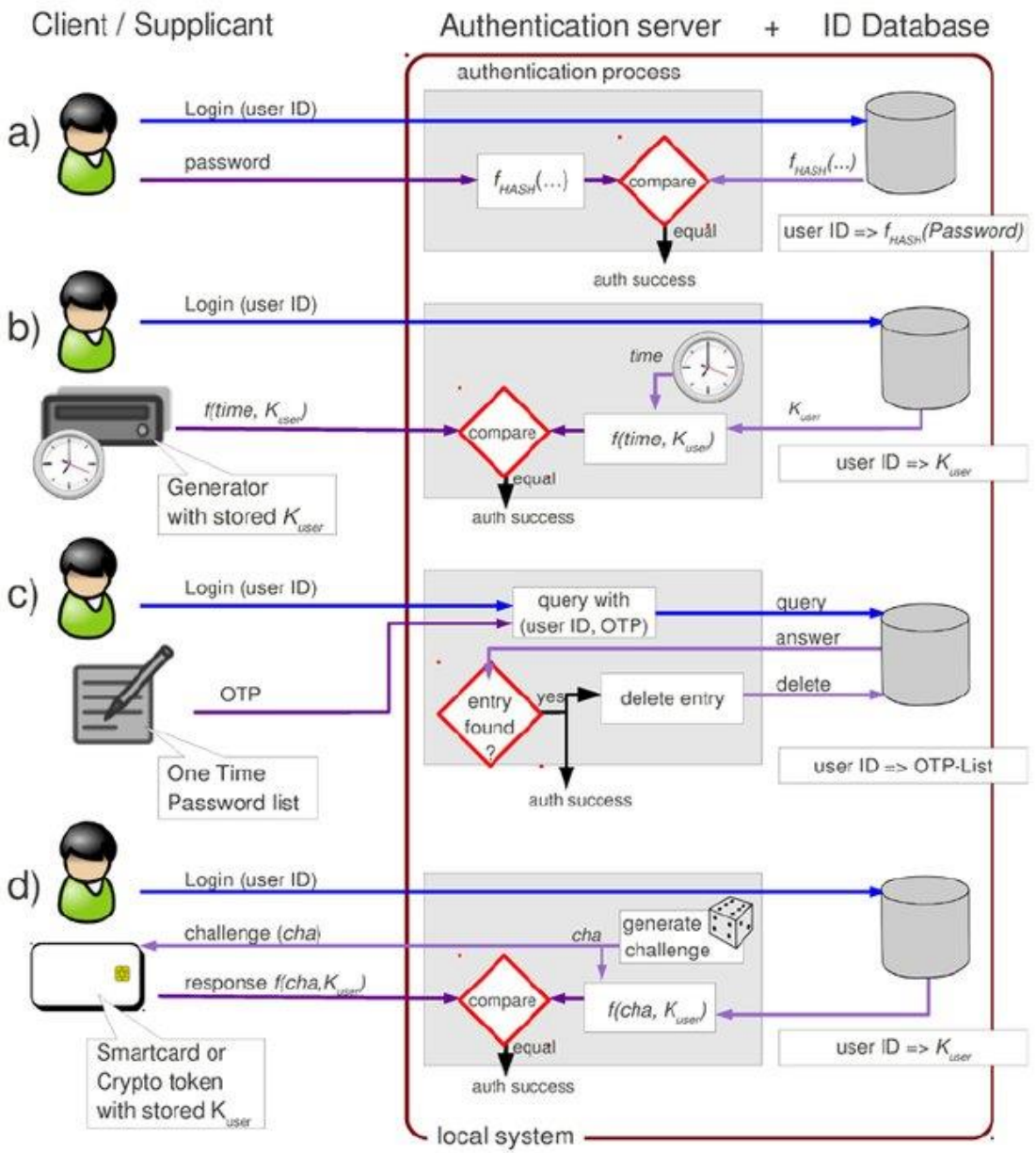
Sursa: Mohammed, Alzahraa & Yassin, Ali adil. (2019). Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device. Cryptography. 3. 24. 10.3390/cryptography3030024.

Ideea de bază din spatele procesului de autentificare bazat pe mai mulți factori



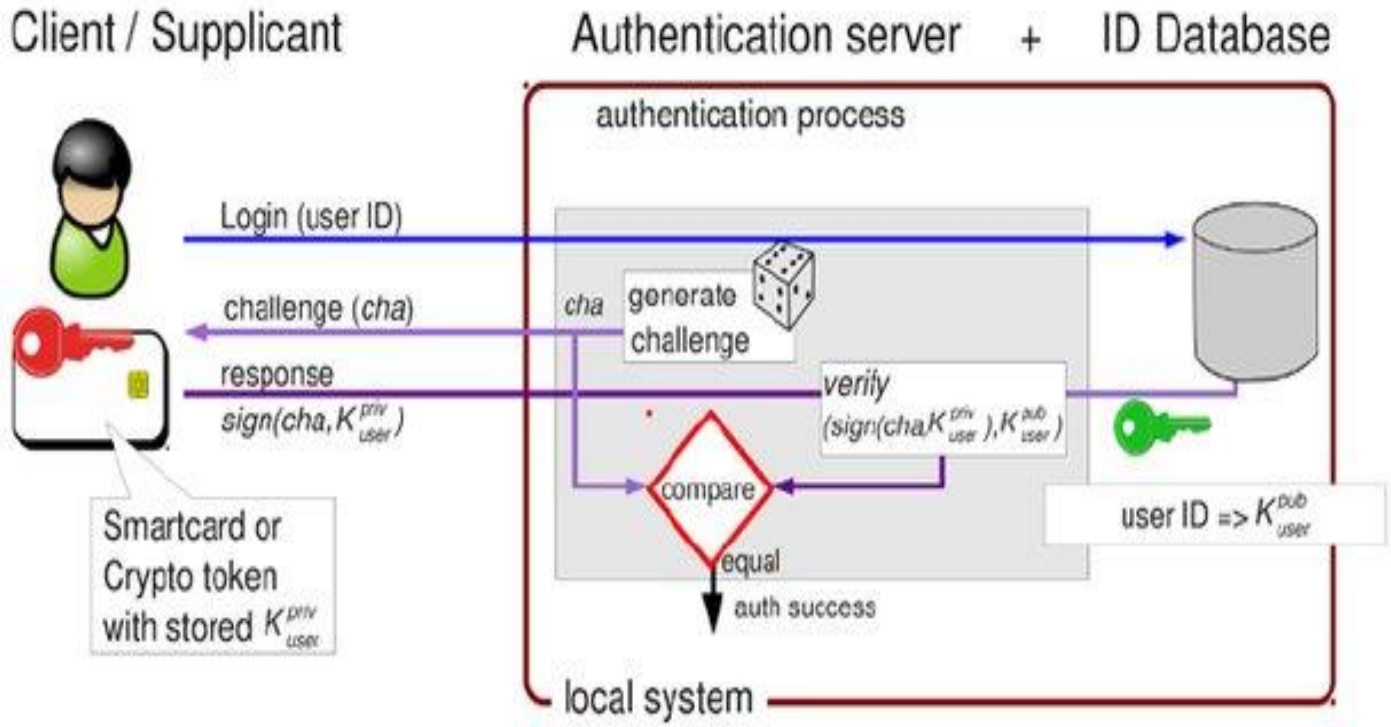
Sursa: Wefel, Sandro & Molitor, Paul. (2012). User Acceptance of Token based Authentication by Single Sign-On. International Journal of Information and Computer Science. 1. 070-077.

Schemă de autentificare locală



Sursa: Wefel, Sandro & Molitor, Paul. (2012). User Acceptance of Token based Authentication by Single Sign-On. International Journal of Information and Computer Science. 1. 070-077.

Autentificarea folosind algoritmi de semnătură și cheie asimetrică



Sursa: Wefel, Sandro & Molitor, Paul. (2012). User Acceptance of Token based Authentication by Single Sign-On. International Journal of Information and Computer Science. 1. 070-077.

Algortmi de semnătură (Signature Algorithms)

- O semnătură digitală este o schemă matematică pentru verificarea autenticității mesajelor digitale sau documente.
- O semnătură validă, în care cerințele necesare sunt îndeplinite, oferă destinatarului un motiv foarte întemeiat și puternic pentru care are posibilitatea să creadă că mesajul a fost creat de către un expeditor cunoscut (autenticitate), și că mesajul nu a most alterat în procesul de trimitere (integritate).
- Semnăturile digitale sunt elemente/componente standard ale suitelor de protocoale criptografice, și de cele mai multe ori sunt întâlnite în:
  - Aplicații software distribuite
  - Tranzacții financiare
  - Aplicații software pentru managementul contractelor.
- O schemă pentru semnătură digitală, tipic, constă în trei algoritmi:
  - Algoritmul pentru generarea cheii care selectează cheia privată în mod aleator și distribuit unifrom dintrun set de chei private posibile.
    - Algoritmul generare cheia privată și o cheie publică.
  - Algoritmul de semnare care produce semnătura pe baza mesajului și cheii private.
  - Algoritmul de verificare al semnăturii care pe baza mesajului, cheii publice și semnăturii, fie acceptă fie respinge autentifcitatea mesajului.

Formalitatea algoritmilor de semnătură

- Formal, schema pentru semnăturile digitale este reprezentată prin trei algoritmi probabilistici polinomiali în timp (PPT – probabilistic polynomial time).
- Acest triplet de algoritmi îl vom nota ca fiind (Gen, Sgn, Ver), îndeplining pe rând următoarele:
  - Gen– reprezintă generatorul de chei, generează o cheie publică k_{pub} și o cheie privată corespondentă k_{prv}, pentru datele de intrare 1^{λ}, unde λ reprezint[parametrul de Securitate.
  - Sgn – returnează un tag, t, pentru datele de intrare: k_{prv} și un șir de caractere (x)
  - Vrf – returnează $acceptat$ sau $respins$ pentru datele de intrare: k_{pub}, x, și t.
- Corectitudinea se calculează astfel încât Sgn și Vrf să indeplinească următoarea probabilitate

$$\Pr\left[(pub_k, prv_k) \leftarrow Gen\left(1^{\lambda}\right), Vrf\left(pub_k, x, Sgn(prv_k, x)\right) = acceptat\right] = 1$$

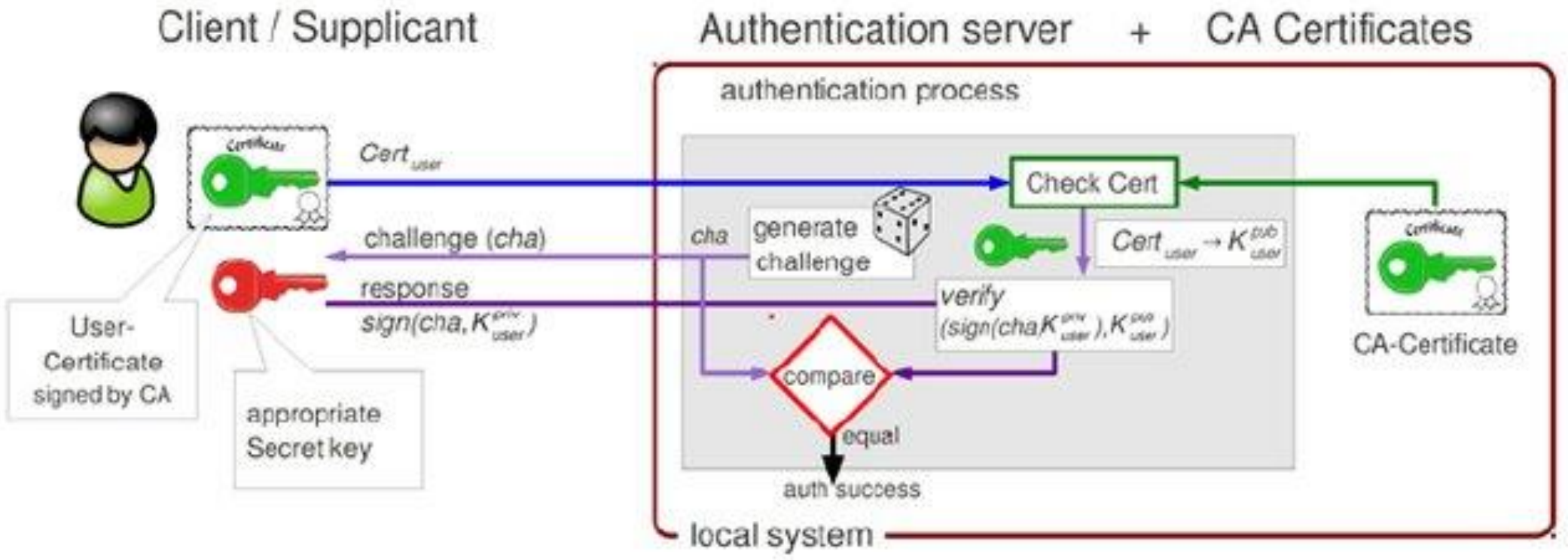
- O semnătură digitală este sigură dacă pentru fiecare adversar probablistic polinomiam non-uniform, Adv.

$$\Pr\left[(pub_k, prv_k) \leftarrow Gen\left(1^{\lambda}\right), (x,t) \leftarrow Adv^{Sgn(prv_k,\cdot)}\left(pub_k, 1^{\lambda}\right), \quad x \notin Q, \quad Vrf(pub_k, x, t) = acceptat\right] < negl(n),$$

unde:

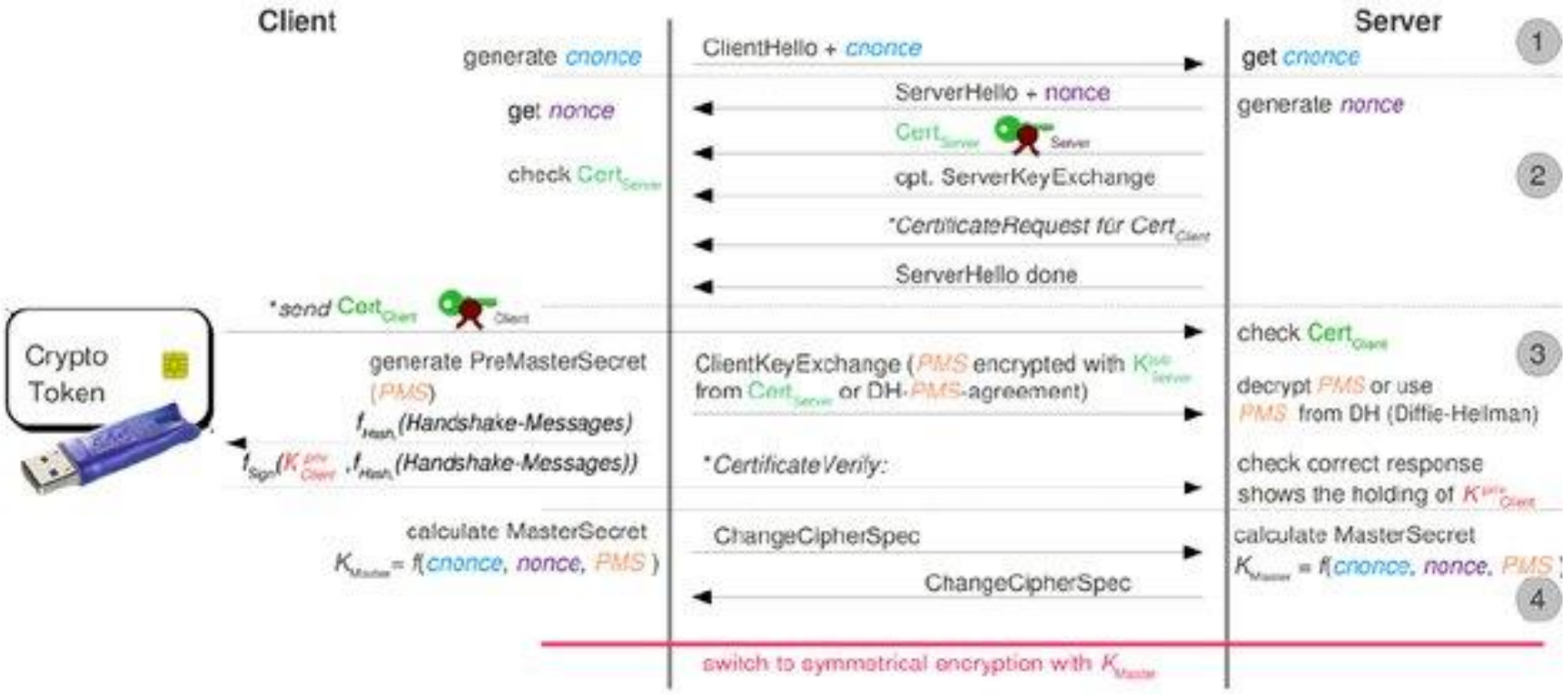
- $Adv^{Sgn(prv_k,\cdot)}$ reprezinta că Adv are acces la oracolul $Sgn(prv_k,\cdot)$
- Q reprezintă un set de interogări realizate pe Sgn efectuate de Adv, care cunoaște pub_k și parametrul de securitate λ, și
- $x \notin Q$ reprezintă adversarul care nu poate realiza interogare directă asupra șirului de caractere, x, pe Sgn.

Autentificarea bazată pe criptografie asimetrică



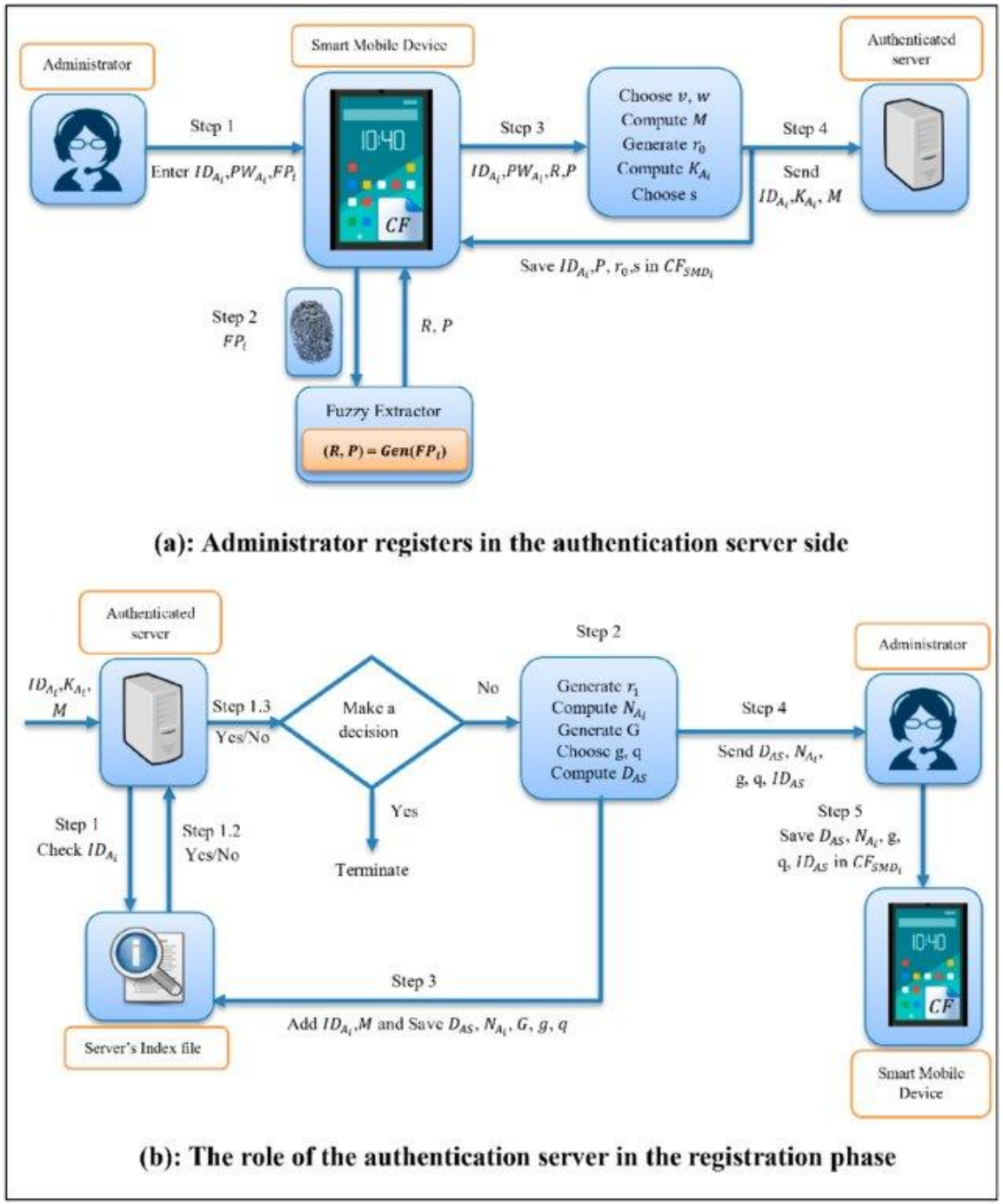
Sursa: Wefel, Sandro & Molitor, Paul. (2012). User Acceptance of Token based Authentication by Single Sign-On. International Journal of Information and Computer Science. 1. 070-077.

Stabilirea unei conexiuni SSL/TLS folosind token criptografic pentru autentificare



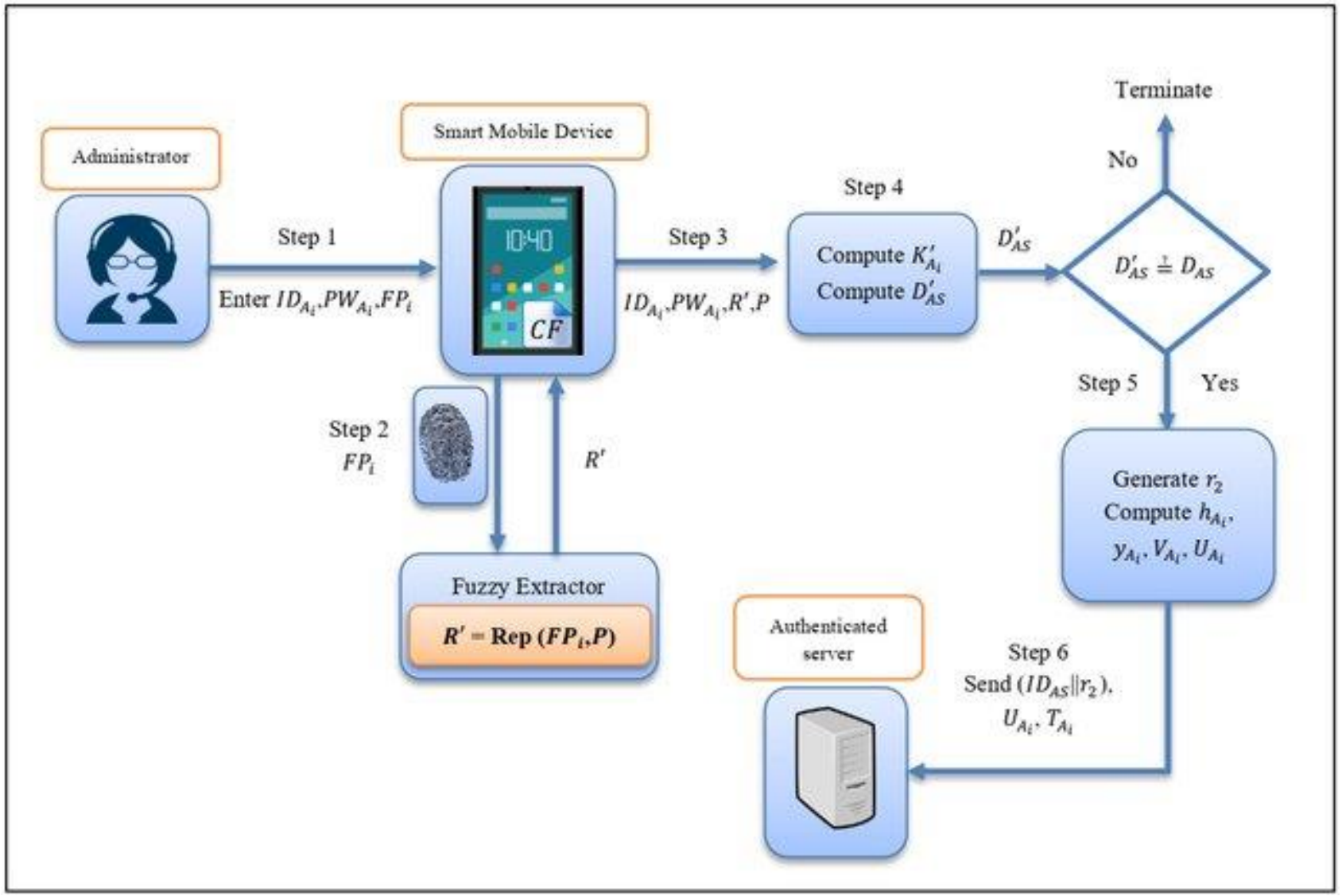
Sursa: Wefel, Sandro & Molitor, Paul. (2012). User Acceptance of Token based Authentication by Single Sign-On. International Journal of Information and Computer Science. 1. 070-077.

Faze de înregistrare - Exemplu



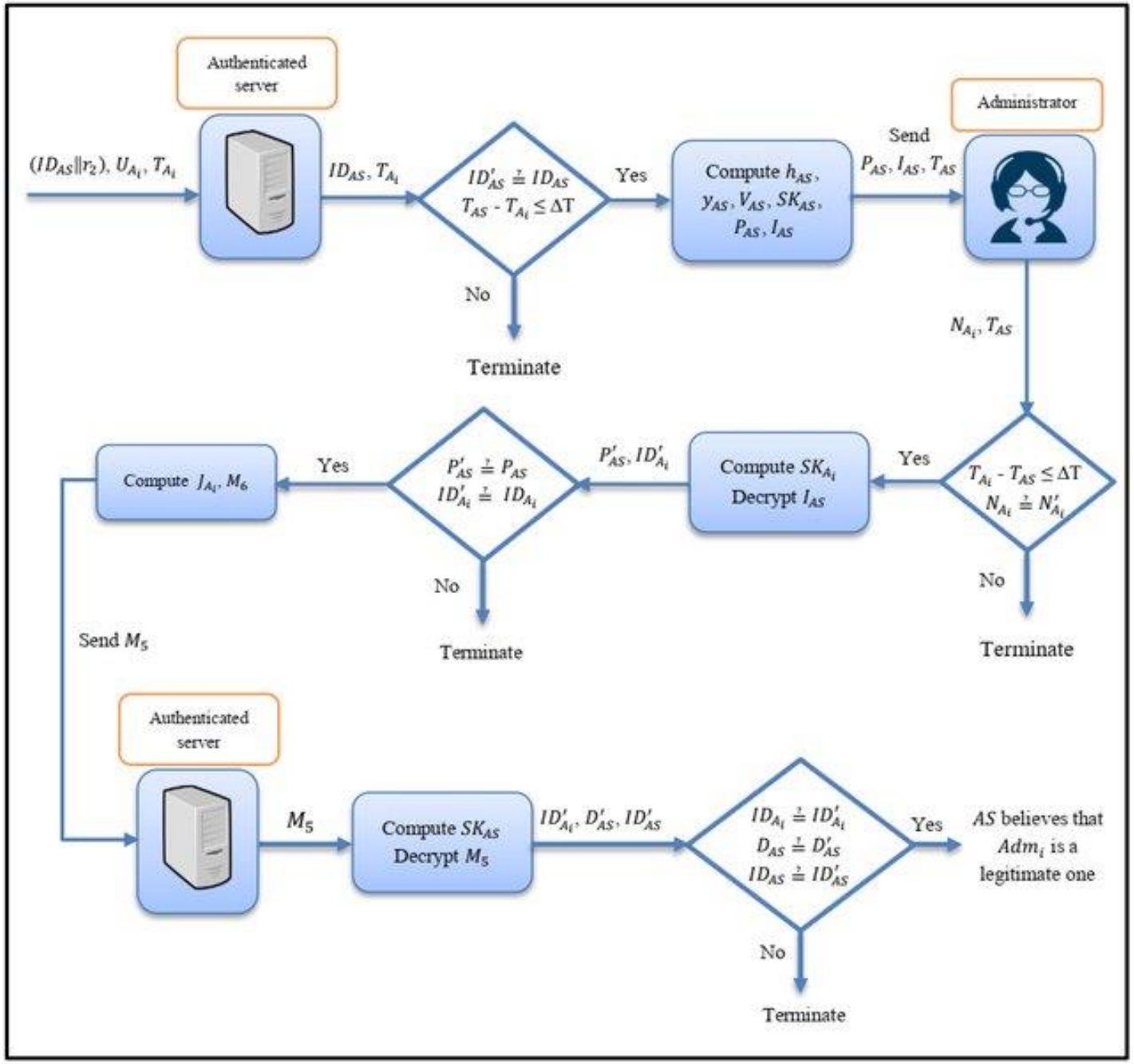
Sursa: Mohammed, Alzahraa & Yassin, Ali adil. (2019). Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device. Cryptography. 3. 24. 10.3390/cryptography3030024.

Faze de autentificare - Exemplu



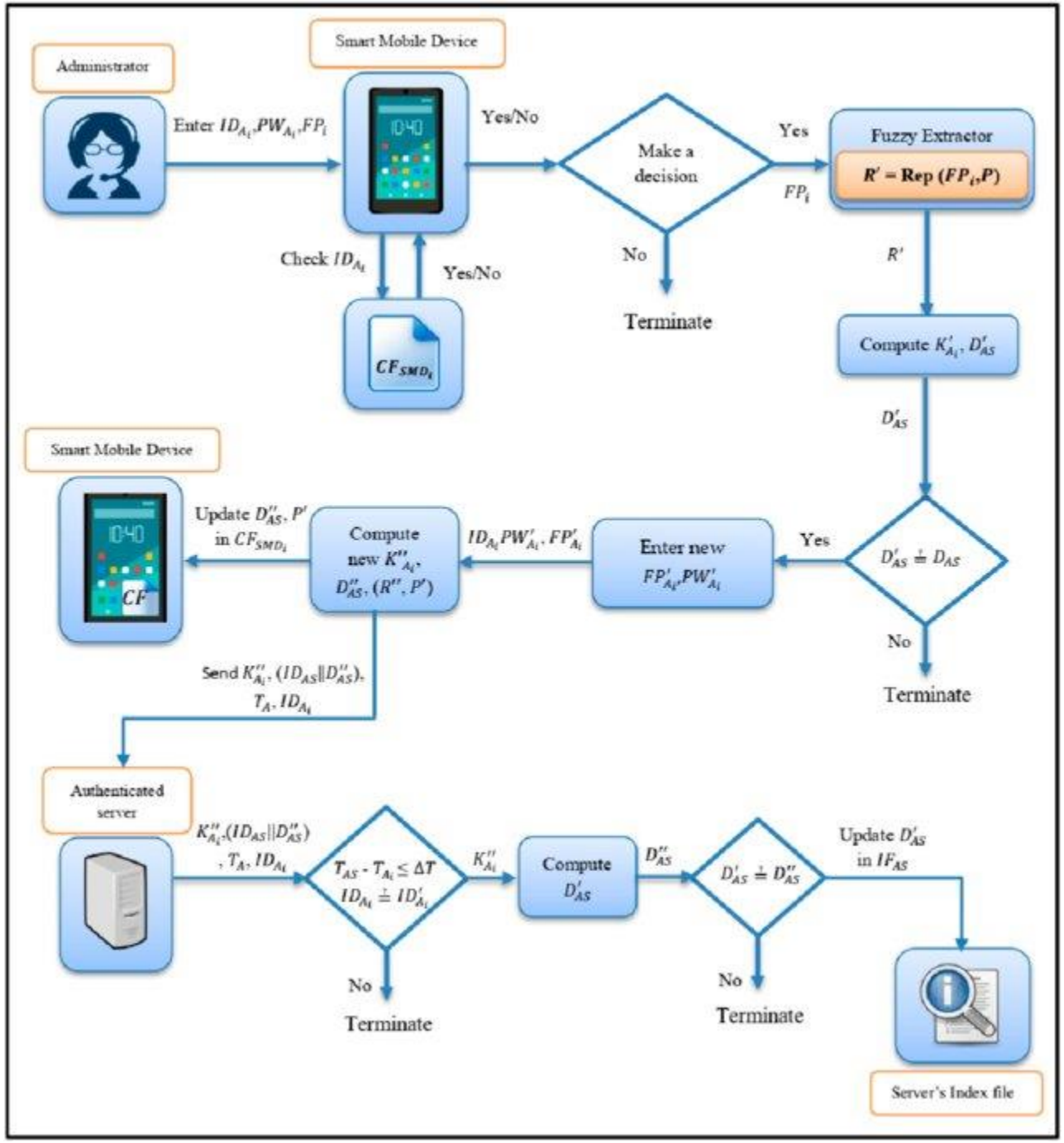
Sursa: Mohammed, Alzahraa & Yassin, Ali adil. (2019). Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device. Cryptography. 3. 24. 10.3390/cryptography3030024.

Procesul de autentificare între serverul de autentificare și adminsitrator



Sursa: Mohammed, Alzahraa & Yassin, Ali adil. (2019). Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device. Cryptography. 3. 24. 10.3390/cryptography3030024.

Procesul de schimbare al parolei



Sursa: Mohammed, Alzahraa & Yassin, Ali adil. (2019). Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device. Cryptography. 3. 24. 10.3390/cryptography3030024.

Avantaje

- Fără token-uri adiționale necesare deoarece utilizează dispozitive mobile care se află mereu asupra utilizatorului.
- Datorită schimbării constante, codurile generate în mod dinamic sunt mai sigure în a fi folosite comparativ cu cele statice.
- În funcție de soluție, codurile care au fost folosite sunt înlocuite în mod automat cu scopul de a asigura că un cod valid este disponibil întotdeauna.

Dezavantaje

- Utilizatorii put fi susceptibili la atacuri de tip phishing .
- Un atacator poate trimite un mesaj text care face legătura cu un site tip *spoofing* care arată identic cu site-ul original/oficial.
- Atacatorul poate obține codul de autentificare și credențialele utilizatorului.
- Uneori – telefonul nu este întotdeauna disponibil – poate fi pierdut, furat, fără baterie, sau alte defecțiuni.
- Clonarea SIM-urilor oferă posibilitatea hackerilor să acceseze conexiunile telefoanelor mobile.
- Atacurile de tip social-engineering asupra operatorilor de telefonie mobilă au scos la iveală foarte multe duplicate ale cardurilor SIM.
- Mesajele text între telefoane folosind SMS sunt destul de nesigure, acestea fiind uneori foarte ușor de interceptat de către IMSI-catcher - International Mobile Subscriber Identity-Catcher, este un dispozitiv care "trage cu urechea" (eavesdropper) utilizat pentru interceptarea traficului telefoanelor mobile și urmărirea datelor referitoare la locație sau la utilizatorii telefoanelor mobile.
- Recuperea conturilor de cele mai multe ori evită procesul de autentificare în doi factori sau cu mai mulți factori.
- Smartphone-urile moderne sunt folosite atât pentru primirea e-mail-urilor cât și SMS-urilor. Dacă telefonul este pierdut sau furta și nu este protejat corespunzător prin intermediul unei parole sau caracteristici biometrice, toate conturile pentru care e-mail-ul este cheia poate fi spart, deoarece telefonul este dispozitivul care primește al doilea factor sau unul dintre factori.

Problema Identității

O problemă de integritate

Problema phishing-ului

Creșterea cererii de utilizare foarte mare pentru autentificarea bazată pe factori multipli

APT13 (Zirconium) ZIRCONIUM

ZIRCONIUM is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community.[1][2]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1583	.001	Acquire Infrastructure: Domains	ZIRCONIUM has purchased domains for use in targeted campaigns.[1]
		.006	Acquire Infrastructure: Web Services	ZIRCONIUM has used GitHub to host malware linked in spearphishing e-mails.[3][4]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ZIRCONIUM has created a Registry Run key named `Dropbox Update Setup` to establish persistence for a malicious Python binary.[4]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	ZIRCONIUM has used a tool to open a Windows Command Shell on a remote host.[4]
		.006	Command and Scripting Interpreter: Python	ZIRCONIUM has used Python-based implants to interact with compromised hosts.[3][4]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	ZIRCONIUM has used a tool to steal credentials from installed web browsers including Microsoft Internet Explorer and Google Chrome.[4]
Enterprise	T1140		Deobfuscate/Decode Files or Information	ZIRCONIUM has used the AES256 algorithm with a SHA1 derived key to decrypt exploit code.[2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	ZIRCONIUM has used AES encrypted communications in C2.[4]
Enterprise	T1041		Exfiltration Over C2 Channel	ZIRCONIUM has exfiltrated files via the Dropbox API C2.[4]

Sursa: https://attack.mitre.org/groups/G0128/

Bibliografie

1. Burt, T. (2020, September 10). New cyberattacks targeting U.S. elections. Retrieved March 24, 2021.
2. Itkin, E. and Cohen, I. (2021, February 22). The Story of Jian – How APT31 Stole and Used an Unknown Equation Group 0-Day. Retrieved March 24, 2021.
3. Huntley, S. (2020, October 16). How We're Tackling Evolving Online Threats. Retrieved March 24, 2021.
4. Singh, S. and Antil, S. (2020, October 27). APT-31 Leverages COVID-19 Vaccine Theme and Abuses Legitimate Online Services. Retrieved March 24, 2021.