**ROMÂNIA**

**MINISTERUL APĂRĂRII NAŢIONALE**

**ACADEMIA TEHNICĂ MILITARĂ**

**„Ferdinand I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Securitate Tehnologiei Informației**



**Aplicație pentru extragerea si indexarea conținutului din documente scanate**

COORDONATOR ȘTIINȚIFIC: ABSOLVENT:

**Col. Prof. univ. Dr. Ing. Mihai TOGAN Slt. Ing. Alin-Romeo TUDOSE**

Conține \_\_\_\_\_\_\_\_\_\_\_ file Inventariat sub nr. \_\_\_\_\_\_

Poziția din indicator: \_\_\_\_

Termen de păstrare:\_\_\_\_\_

**BUCUREȘTI**

**2023**

PAGINĂ ALBĂ

PAGINA ALBA

PAGINĂ ALBĂ

PAGINĂ ALBĂ

PAGINĂ ALBĂ

PAGINĂ ALBĂ

# ABSTRACT

# REZUMAT

**Cuprins**

[ABSTRACT 7](#_Toc126173416)

[REZUMAT 8](#_Toc126173417)

[LISTĂ ABREVIERI 10](#_Toc126173418)

[LISTĂ FIGURI 11](#_Toc126173419)

[INTRODUCERE 12](#_Toc126173420)

[1.1. Importanța și actualitatea problematicii abordate 12](#_Toc126173421)

# LISTĂ ABREVIERI

|  |  |  |
| --- | --- | --- |
| **Nr. Crt** | **Abreviere** | **Forma completă** |
| 1. | PKI | Public Key Infrastructure (Infrastructură cu chei publice) |

# LISTĂ FIGURI

**No table of figures entries found.**

CAPITOLUL I

# INTRODUCERE

## Importanța și actualitatea problematicii abordate

Nevoia de securitate este o constantă a lumii moderne, în care tot mai multe sarcini umane sunt preluate de către calculator. Informațiile comunicate de sistemele informatice sunt din ce mai sensibile, iar compromiterea acestora poate genera daune foarte mari de ordin financiar în organizațiile civile sau vulnerabilități de securitate națională în organizațiile militare.

Pentru prevenirea scurgerilor de informații, sau modificarea ilicită a documentelor de importanță crescută, au fost adoptate pe scară largă servicii criptografice care au scopul de a ascunde și de a garanta integritatea și autenticitatea datelor transmise între două entități, folosind mecanisme criptografice precum criptarea, semnăturile digitale și certificatele digitale.

Desigur, în utilizarea certificatelor și a semnăturilor digitale apare o mare întrebare. Cum putem avea încredere că un certificat este valid, și că entitatea care deține acel certificat este cine spune că este? Pentru a rezolva acest impediment, au fost implementate scheme de certificate diferite, precum Web of Trust, sau PKI.

În implementarea schemei PKI, certificatele digitale sunt emise și gestionate de către terțe părți specializate, care sunt marcate ca puncte de încredere în sistemul folosit. Cu alte cuvinte, nu se rezolvă complet problema încrederii, deoarece trebuie să avem încredere *„oarbă”* în acele terțe părți.

Așadar, pentru a aduce un plus de securitate schemei, a fost introdusă componenta legislativă în cadrul schemelor de securitate, de către un corp autorizat de reglementare, și anume Comisia Europeană. Aceasta certifică furnizorii de servicii de securitate care oferă servicii conforme cu standardul eIDAS, din spațiul Uniunii Europene, precum și al Spațiului Economic European.