



Tehnologie pentru o lume mai sigură

**Servicii de încredere în
securitatea comunicațiilor**

Ziua Comunicațiilor

SERVICII DE ÎNCREDERE

- **Serviciul de încredere reprezintă acel serviciu care, utilizând tehnologii criptografice, oferă uneia sau mai multor entități încredere în utilizarea sistemelor informatice.**
- **Accelerează adoptarea activităților electronice**
- **Oferă siguranță interacțiunilor de afaceri**

SCHEME DE ACREDITARE

- ***schemă*** - proces organizat de
 - supervizare,
 - monitorizare,
 - aprobare
 - orice altfel de practici
- **Scopul** - să asigure faptul că se îndeplinesc criteriile specifice pentru a se menține încrederea în anumite servicii oferite de un furnizor de servicii de încredere

SCHEME DE ACREDITARE

- **Furnizarea de informații legate de starea unui furnizor de servicii de încredere (FSI)**
- **referințe la criteriile pe care FSI trebuie să le satisfacă pentru a fi acreditat conform unei scheme**
 - **responsabilitatea financiară**
 - **menținerea listelor cu elemente revocate,**
 - **data ultimului audit,**
 - **raportul cu incidentele de securitate**

SCHEME DE ACREDITARE

- **schemele au stabilit proceduri de furnizare a informațiilor despre starea FSI**
- **Schemele, protocoalele, formatele utilizate nu sunt compatibile pentru obținerea acestor informații despre terțele părți**
- **necesitatea compatibilizării schemelor existente și propunerea unui model de referință**

TIPURI DE SCHEME DE ACREDITARE

- ***schemă impusă*** este acea schemă creată de guvernul unei țări cu scopul de a se respecta legile și normele din domeniu (ex. Directiva Europeană)
- **schemele impuse - administrate de un organ guvernamental**
- **guvernul poate să subcontracteze administrarea schemelor impuse unei firme private**

TIPURI DE SCHEME DE ACREDITARE

- ***schemele voluntare***- scheme create și administrate de organisme private
- **guvernul poate să participe atât la crearea cât și la administrarea unei astfel de scheme voluntare**
- **o schemă voluntară poate ajuta la controlul modului de îndeplinire a cerințelor legale**
- **schemele voluntare sunt la rândul lor împărțite în scheme voluntare publice și scheme voluntare private, în funcție de măsura în care guvernul este implicat în crearea și administrarea acestor scheme**

SCHEME DE ACREDITARE ADOPTATE

Zona	Numele țării	Codul țării (ISO 3166-1)	Schemă impusă	Schemă voluntară	
				Publică	Privată
EU	Austria	AT	✓	✓	
	Belgia	BE	✓	✓	
	Germania	DE	✓	✓	
	Danemarca	DK	✓		
	Spania	ES	✓	✓	
	Finlanda	FI	✓		
	Franta	FR	✓		
	Marea Britanie	GB	✓		Scheme
	Grecia	GR	✓	✓	
	Irlanda	IE	✓		NAB
	Italia	IT	✓		
	Olanda	NL	✓		TTP.NL
	Portugalia	PT	✓		
	Suedia	SE	✓		
Europa (alte țări)	Elveția	CH	✓		
	Norvegia	NO	✓		NA
Alte Regiuni	Ungaria	HU	✓		
	Australia	AU	✓		
	Australia/ Noua Zeelandă	AU/NZ			CFA
	Canada	CA			WebTrust
	SUA	US			WebTrust Identity

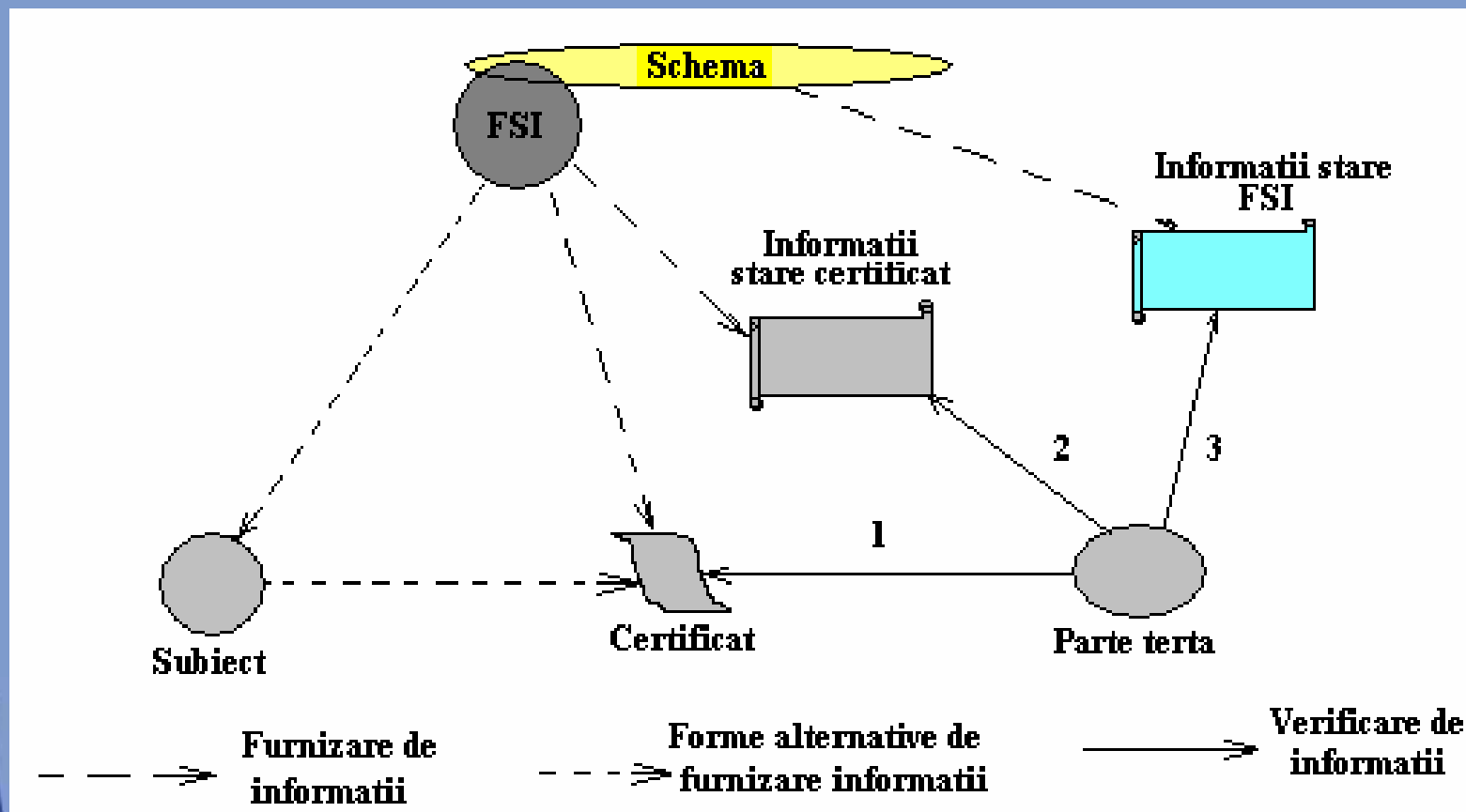
CARACTERISTICILE SCHEMELOR DE ACREDITARE

- **supervizați toți FSI, indiferent de serviciile oferite (AT, DE, ES)**
- **sunt supervizați numai furnizorii de servicii de certificare (BE, CH, DK, FI, FR, GB, HU, IE, IT, NL, NO, PT)**
- **Tipuri de supervizari:**
 - **reacțiune (GB)**
 - **notificare cu publicare (FR)**
 - **notificare cu interzicere (ES, NO)**
 - **notificare și verificarea documentației (AT, BE, DE, FI, IE, NL)**
 - **testare și aprobare (CH, HU, IT)**

MODEL DE ÎNCREDERE

- **Încrederea în mediul deschis (public) care ofera un serviciu de încredere este construită pe baza urmatorilor factori:**
 - **setul de cerințe legate de acel serviciu să fie bine cunoscut și agreeat**
 - **criteriile de aprobare a acelui serviciu utilizate de evaluatori/auditori să fie compatibile**
 - **mijloacele de transmitere a informațiilor despre FSI să fie de asemenea compatibile**

MODEL DE INCREDERE



MODEL DE INCREDERE

- **există o parte statică a informațiilor care oferă imaginea despre starea unui FSI și o parte dinamică**
- **partea statică se bazează pe rezultatele evaluării inițiale a FSI, făcute conform unei scheme.**
- **partea dinamică se bazează pe:**
 - **rezultatele unui audit periodic**
 - **evenimente raportate de procese specifice schemei cum ar fi: schimbări ale stării financiare a FSI care influențează responsabilitate FSI, incidente de securitate etc**

MODEL DE ÎNCREDERE

- **Exista o serie de mecanisme de consultarea stării unui FSI**
- **Liste semnate: Italia, Marea Britanie (tScheme), WebTrust.**
- **Certificate de aprobare:**
 - **pentru un FSI, la fiecare serviciu aprobat se asociază o marcă de aprobare.**
 - **tScheme si WebTrust**
 - **dezavantaj: nu se poate păstra un istoric al stărilor FSI.**
- **Lanțuri de încredere:**
 - **există un punct de încredere, începând de la care se poate parcurge un lanț de încredere pentru a se determina membrii unei scheme.**
 - **dezavantaj: nu se poate păstra un istoric al stărilor FSI.**
- **Liste “albe/negre”:**
 - **au același dezvantaj**
 - **“Lista neagră” se bazează pe presupunerea că absența din această listă indică conformitatea cu cerințele schemei**

SERVICII DE INCREDERE IN ROMANIA

- **Legea semnăturii electronice este în conformitate cu Directiva UE și elementul central este conceptul de certificat calificat**
- **Rezultă că în România există o schemă impusă, deoarece se arată că în fața legii au valoare numai semnăturile extinse, adică cele create pe baza certificatelor calificate**
- **Conform Normelor metodologice, s-a înființat *Autoritatea de Reglementare și Supraveghere (ARS)*, care elaborează reglementări privind funcționarea furnizorilor de servicii de certificare și supraveghează operarea corectă în domeniu**

SERVICII DE INCREDERE IN ROMANIA

- **ARS păstrează o evidență a FSC publici (atât pentru certificate calificate, cât și necalificate) într-un registru electronic de evidență semnat care trebuie să fie disponibil**
- **este necesar ca formatele și protocoalele să fie în conformitate cu cele propuse de ETSI pentru a se da posibilitatea unei terțe părți (din țară sau din străinătate) să poată determina starea unui anumit furnizor de servicii de certificare**
- **sunt necesare regulamente de funcționare și specificarea concretă a cerințelor de acreditare a furnizorilor de servicii de certificate (cerințe privind securitatea operațiilor, omologarea dispozitivelor de creare de semnătură etc.)**
- **ARS, conform normelor metodologice, nu poate ține evidența decât a furnizorilor de servicii de certificare**

CONCLUZII

- **Armonizarea schemelor de acreditare – element necesar pentru realizarea unei rețele de încredere globale**
- **PKI este suportul principal pentru serviciile de încredere**
- **Serviciile de marcă temporală și validare a certificatelor digitale sunt servicii de încredere importante și trebuie creat cadrul legal și pentru functionarea și supervizarea acestora**
- **Produsele de securitate dezvoltate de UTI indeplinesc condițiile impuse de schema de acreditare și pot fi utilizate cu succes de orice furnizor de servicii de încredere inclusiv pentru marcare temporală și validarea certificatelor**