

TEMA 1 – D.A.T.C

- **Protocolul HTTPS (Hypertext Transfer Protocol Secure)**
 - Este o extensie a protocolului **HTTP (Hypertext Transfer Protocol)** pentru o comunicare securizata in cadrul unei retele.
 - Protocolul de comunicare este **criptat** cu ajutorul **TLS (Transport Layer Security)** sau cu ajutorul predecesorului **SSL (Secure Sockets Layer)**
 - **HTTPS** este o metoda de autentificare a server-ului web care il foloseste, prin intermediul asa-numitelor “**certificate digitale**” - o colectie de date pe care un browser o solicita server-ului pentru a putea incepe transferul criptat;
 - Daca certificatul digital este emis de catre o autoritate cunoscuta, browser-ul poate fi sigur ca server-ul cu care comunica este ceea ce pretinde a fi.
 - **HTTPS nu trebuie** confundat cu **Secure HTTPS(S-HTTP)**
- **SOA (Service Oriented Arhitecture)**
 - Este un tip de arhitectura software care presupune distribuirea functionalitatii aplicatiei in unitati mai mici, distincte, numite servicii, care pot fi distribuite intr-o retea si pot fi utilizate impreuna pentru a crea aplicatii desinate afacerilor.
 - Aceste servicii au o capacitate mare de a fi reutilizare in aplicatii diferite
 - Aceste servicii comunica intre ele triminand informatii de la un serviciu la altul.
 - Este o arhitectura flexibila si standardizata ce contribuie la o mai buna conectare a diverselor aplicatii si faciliteaza schimbul de informatii
 - SOA unifica procesele de business structurand marile aplicatii intr-o colectie de module mai mici numite servicii.
 - Serviciile sunt unitati functionale neasociate care nu au apeluri unele catre altele inglobate in ele.
- **Acces Token**
 - Acesta contine credentialele de securitate pentru o sesiune de autentificare si identifica userul, grupul user-ului, drepturile user-ului si in unele cazuri o aplicatie particulara
 - Un token de acces este in general folosit doar pentru a reprezenta informatii de securitate, insa acesta este capabil sa retina si informatii suplimentare
 - Acesta este generat de catre **serviciul de logon** atunci cand un user se logheaza in sistem si credentialele user-ului sunt autentificate de catre baza de date
 - Tipuri de tokeni:
 - **Primary token** – Acestia pot fi asociati doar cu procese si reprezinta un obiect de securitate al procesului. Creearea acestui token necesita doua privilegii separate pentru ca acesta sa fie creat.
 - **Impersonation Token** – Este un concept de securitate implementat in Windows NT care permite unei aplicatii server sa fie temporar un client, pentru a accesa obiecte securizate. Acesta are 4 nivele posibile: **Anonymous, Identification, Impersonation, Delegation**