REZUMAT

Documentele electronice cu valoare juridică poate fi utilizate datorită legislației care echivalează semnăturile electronice calificate cu semnăturile olografe. Odată cu intrarea în vigoare a Regulamentului eIDAS, utilizatorii pot aplica semnături electronice calificate fără să dețină fizic un dispozitiv criptografic. În cadrul unui astfel de sistem, cheile private ale utilizatorului sunt generate, stocate și folosite în cloud. Această modificare atrage după sine anumite provocări, dintre care cele mai importante sunt: asigurarea controlului exclusiv al utilizatorului asupra cheilor private stocate în cloud și asigurarea interoperabilității aplicațiilor de semnătură cu serviciile de semnare expuse de furnizorii de servicii de certificare. Principalul avantaj oferit de semnăturile electronice în cloud constă în creșterea mobilității și a uzabilității.

În contextul în care tot mai multe companii și state urmează procese de digitalizare, dezvoltarea domeniului pentru a obține sisteme de semnătură electronică mai sigure și mai ușor de utilizat capătă o importanță semnificativă. Astfel, un obiectiv general al acestei teze este identificarea elementelor care pot fi îmbunătățite, astfel încât semnăturile electronice în cloud să fie mai sigure și mai ușor de utilizat. Mai concret, obiectivele tezei gravitează în jurul noilor infrastructuri pentru semnătură electronică, adresând trei aspecte importante: securitatea, uzabilitatea și modalitățile de utilizare ale semnăturilor electronice în cloud.

Din perspectiva uzabilității, sistemele pentru semnătură electronică în cloud dețin un potențial considerabil, dar care nu este încă fructificat complet. Tranziția de la aplicațiile de semnături locale la semnături în cloud poate fi anevoioasă din două motive: experiența utilizatorului este modificată și aplicațiile trebuie să schimbe implementarea prin care sunt procesate semnăturile. În vederea armonizării standardelor de semnătură electronică locală cu cele pentru semnătură electronică în cloud, sunt propuse în teză două module criptografice software. Acestea permit ca aplicațiile de semnătură compatibile cu PKCS\#11 sau CNG să realizeze semnături electronice în cloud într-un mod transparent, fără a fi necesară nicio modificare în cadrul aplicației.

În ceea ce privește modul de utilizare al semnăturilor în cloud, este de remarcat potențialul de a degreva alte sisteme care gestionează chei private de această sarcină. Astfel, o altă contribuție este identificarea sistemelor care pot beneficia de această facilitate. Din această perspectivă, este propusă modificarea protocoalelor de autentificare bazate pe coduri QR. În acest mod, dispozitivele mobile sunt degrevate de sarcina gestionării cheilor private și protocolul devine mai sigur și mai flexibil.

Din punct de vedere al securității, toate cerințele menționate în legislație și în standarde pot fi rezumate la una singură: cheile private ale utilizatorului se află sub controlul exclusiv al acestuia, chiar dacă ele sunt stocate în cloud. În acest scop, în teză este propusă soluția SABRES. Aceasta oferă utilizatorilor o sursă de încredere distribuită, ce stochează într-o formă imuabilă toate accesările cheilor private și respectă legislația și standardele în vigoare.