Criptografia cu chei în custodie

Prof.dr.Victor-Valeriu PATRICIU
Catedra de Calculatoare, Academia Tehnică Militară, Bucureşti

Conceptul de custodie a cheilor criptografice (Key Escrow) îşi are punctul de plecare în SUA anilor 90', unde s-a încercat impunerea, de către agenţile statului însărcinate cu securitatea naţională, a unui sistem prin care acestea, sub arobare legală, să poată decripta transmisiile în reţele ale unor firme sau persoane. Conceptul rerezintă nucleul central al programului guvernamental Clipper, numit şI Escrowed Encryption Standard(EES), integrat unuia mai larg, numit Capstone. Articolul prezintă o scurtă taxonomie şi o descriere a multor scheme posibile, care extind sistemele de cifrare cu chei în custodie. Se încearcă o trecere în revistă a diferitelor variante de astfel de sisteme şi câteva realizări notabile ce se propun deja spre utilizare.
Cuvinte cheie: *criptografie computaţională, cheie de sesiune, criptare, decriptare forţată, sisteme simetrice de cifrare, semnătură digitală, sisteme cu chei publice, criptare cu chei în custodie.*

1. De ce criptografie cu chei în custodie?

În decursul ultimilor 20 de ani s-a acumulat o anumită tensiune privind interesele publice pentru protecţia informaţiilor şi interesele guvernamentale pentru obţinerea accesului la informaţiile adversarilor. Programul *Clipper Key Escrow* a fost o încercare de depăşire a acestei tensiuni, oferind publicului o criptografie bună, păstrându-se pentru organele de impunere legală abilitatea de a decripta comunicaţiile, când acest lucru este autorizat. În acelaşi timp, atât utilizatorii singulari cât şi organizaţiile se tem de consecinţele pierderii cheilor. Un sistem care ar putea satisface atât cerinţele utilizatorilor singulari şi a corporaţiilor, dar care să îndeplinească şi cerinţele guvernamentale de decriptare autorizată, ar putea rezolva aceas-tă problemă de interes internaţional.

Odată cu apariţia comunicaţiilor electronice, devine posibilă interceptarea convorbirilor fără a putea fi detectată această interceptare. Această capabilitate oferă un avantaj celui care interceptează şi un dezavantaj serios celor spre care este orientată această interceptare. Uneori cel care interceptează este guvernul - un organism abilitat legal sau o agenţie de informaţii - şi aceste agenţii au învăţat să preţuiască foarte mult aceste surse de informaţii. Alteori, cel care intercepteaza este un infractor. În acest caz este necesară o formă adecvată de securitate. Criptografia oferă securitatea dorită iar calculatoarele digitale oferă mijlocul pentru implementarea criptografiei de înaltă calitate, cu inconveniente minime pentru utilizator. Calculatoarele personale au coborât costurile unei asemenea criptografii. Aceasta a dus la o "explozie" în folosirea criptografiei.

Asigurarea confidenţialităţii comunicaţiilor şi a datelor memorate în fişiere sau baze de date devine rapid parte integrantă a infrastructurii noastre informaţionale. Scopul explicit al criptografiei este de a face dificil sau imposibil, pentru o terţă parte, accesul la informaţia protejată. În mod clar, devine o problemă cazul în care această terţă parte este o autoritate a statului, care, din motive legale sau sociale, consideră uneori că are dreptul de acces la această informaţie. Motivaţiile legale sau sociale ale acestui "drept de ascultare" sunt discutabile şi au fost îndelung dezbătute. S-a ajuns la concluzia că avem nevoie de mecanisme care să permită accesul la informaţie a unei terţe persoane autorizate, continuând însă să se protejeze informaţia în faţa altor persoane. Se foloseşte termenul de *criptografie cu chei în custodie* pentru a desemna asemenea sisteme.

În timp ce dezbaterea iniţială a fost dominată de propunerea guvernului SUA - *Escrow Encryption Standard* (*Standardul pentru criptarea cu chei în custodie*), acum există deja câteva sisteme diferite care au fost propuse şi discutate. Aceste metode nu diferă numai prin detaliile tehnice, ci ele

schimbă natura acestui acces autorizat. De exemplu, în timp ce multe scheme permit autorității să recreeze complet cheia secretă pe termen lung, alte soluții permit dezvăluirea cheilor de sesiune de termen scurt. Această diferență ce pare nesemnificativă are consecințe practice importante: concentrarea pe cheile de sesiune permite o mai bună exactitate a controlului, furnizând metode prin care autoritatea poate selecta comunicațiile unui anumit individ, nu însă și pe cele particulare, de exemplu cu soția sa sau cu avocatul.

2. Structura unui sistem criptografic cu chei în custodie

Un sistem criptografic cu chei în custodie (*EES - Escrowed Encryption System*) este un sistem de criptare cu posibilități de decriptare forțată, lucru care permite persoanelor autorizate - utilizatori, membrii unei organizații private sau guvernamentale - sub anumite condiții prestabilite, să decripteze criptotextul cu ajutorul informației furnizate de una sau mai multe părți ce dețin anumite chei speciale de recuperare a datelor. Cheile de recuperare a datelor nu sunt, în mod normal, aceleași cu cele folosite pentru criptarea și decriptarea informațiilor ci furnizează tocmai un mijloc pentru determinarea acestor chei de criptare și decriptare. Termenul *criptografie cu chei în custodie* este folosit pentru a referi protecția acestor chei în vederea recuperării datelor. Un sistem criptografic cu chei în custodie poate fi divizat în trei componente principale:

- **USC** (User Security Component) este un dispozitiv hardware sau un program software care oferă capabilități de criptare-decriptare precum și suport pentru funcțiile de custodie a cheilor. Acest suport poate include atașarea unui câmp pentru recuperarea datelor-DRF (*Data Recovery Field*). DRF poate fi parte a mecanismului de distribuție a cheilor.
- **KEC** (Key Escrow Component). KEC, cu care operează agenții pentru custodia cheilor (*Key Escrow Agents*), este răspunzător cu memorarea și eliberarea (folosirea) cheilor pentru recuperarea datelor. Poate fi parte a sistemului de gestiune a certificatelor pentru chei publice sau a infrastructurii generale de gestiune a cheilor.
- **DRC** (Data Recovery Component) constă din algoritmi, protocoale și echipamentul necesar pentru obținerea textului clar din textul criptat și din informațiile conținute în DRC, furnizate de KEC. Această componentă este activă numai atunci când este necesară o recuperare autorizată de date (decriptare forțată).

Figura 1 arată interacțiunea acestor componente. USC criptează datele cu o cheie K și atașează un DRF la textul criptat. DRC reface datele inițiale folosind informația conținută în DRF plus informația furnizată de KEC.

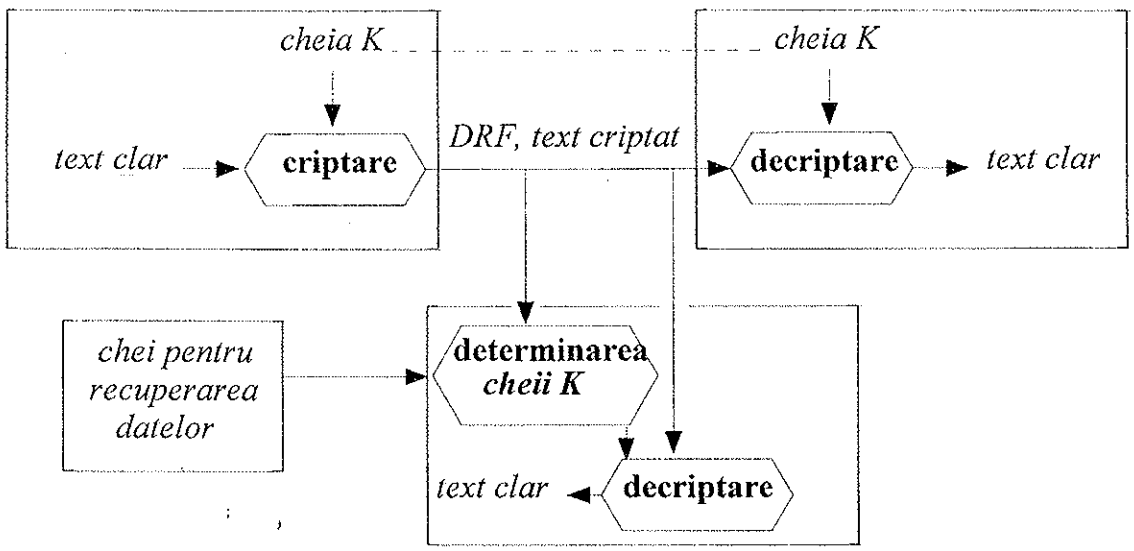

Fig. 1. Sistem criptografic cu chei în custodie

3. Componenta de securitate a utilizatorului (USC)

USC criptează şi decriptează datele şi îndeplineşte funcţiile pentru crearea suportului pentru o eventuală recuperare a datelor. Este caracterizat de următoarele:

• **Domeniul aplicaţiei**. USC poate accepta unul sau ambele din următoarele domenii:

- *Comunicaţii*. Acestea includ convorbirile telefonice, poşta electronică şi orice alt fel de conexiuni. Decriptarea forţată se face prin impunere legală, însoţită de un mandat autorizat de interceptare a comunicaţiilor.
- *Memorarea datelor*. Datele memorate pot fi simple fişiere sau obiecte mult mai generale. Decriptarea forţată este folosită atât de către proprietarul datelor, pentru recuperarea cheilor pierdute sau deteriorate, cât şi prin impunere legală, pentru decriptarea fişierelor care fac obiectul unui mandat autorizat de o instanţă legală.

• **Algoritmul de criptare a datelor**. Următoarele atribute sunt relevante pentru criptarea cu chei în custodie :

- *Numele algoritmului şi modul de operare*. Modul de operare poate afecta exportabilitatea sistemului (de exemplu în SUA, modurile de criptare triplă nu sunt acceptate în cadrul unei licenţe de export).
- *Lungimea cheii*. De asemenea, poate afecta exportabilitatea.
- *Clasificarea*. Un algoritm poate fi clasificat secret sau nesecret; dacă este nesecret poate fi proprietatea unei firme sau poate fi public.

• **Identificatorii şi cheile memorate**. USC memorează identificatori şi chei pentru decriptarea forţată:

- *Identificatorii* se referă la USC sau utilizator, identificatori pentru chei şi identificatori pentru KEC sau agenţi de custodie.
- *Chei*. Pot cuprinde chei unice pentru USC, chei aparţinând utilizatorului sau chei globale de sistem, folosite de KEC. Acestea pot fi publice sau private. Copii ale cheilor sau corespondentele lor private pot fi păstrate în custodie.

• **Mecanismul DRF**. Când datele sunt criptate cu cheia K, USC trebuie să lege textul criptat şi cheia K de una sau mai multe chei de recuperare, prin ataşarea un DRF la date criptate. Legătura este caracterizată prin:

- *Cui aparţin cheile de recuperare*. K poate fi legată cu cheile deţinute de agenţii de custodie ai expeditorului, ai destinatarului sau ai ambilor. Alegerea afectează recuperarea datelor.
- *Rolul în cadrul mecanismului de distribuţie*. DRF şi mecanismul de legare pot fi integrate în protocoale folosite pentru transmiterea cheii K destinatarului dorit. În acest caz, expeditorul trebuie să transmită un DRF valid pentru ca destinatarul să obţină cheia.
- *Conţinutul DRF*. În mod normal DRF conţine cheia K, criptată cu una sau mai multe chei de recuperare (de exemplu, o cheie produs, cheia publică a expeditorului sau a destinatarului sau o cheie publică master a KEC). În unele cazuri numai o parte din biţii cheii K pot fi disponibili prin DRF, restul trebuind să fie determinaţi prin căutare brută (exhaustivă). De asemenea, DRF conţine informaţii ce identifică cheile pentru recuperarea datelor, KEC sau agenţii de custodie, modul şi algoritmul de criptare sau metoda de creare a DRF. Întregul DRF poate fi criptat folosind o cheie de familie (*Family Key*) asociată cu DRC, pentru a proteja identificatorii transmişi în cadrul DRF. Poate fi folosită atât criptografia cu chei simetrice cât şi cea cu chei publice.
- *Transmisia şi frecvenţa*. În mod normal, DRF precede textul criptat într-un mesaj sau într-un header de fişier. Pentru conexiuni deschise, DRF poate fi retransmis la intervale regulate de timp.
- *Validare*. DRF poate include un autentificator de custodie (*Escrow Authenticator*), verificat de destinatar pentru a determina integritatea DRF. Chiar dacă se folosesc chei publice pentru crearea DRF-ului, destinatarul poate recalcula DRF-ul şi poate compara rezultatul cu DRF-ul primit.

• **Implementarea**. Un USC poate fi implementat hardware, software, firmware sau combinaţii de acestea. Hardware este în

general mai sigur şi mai puţin vulnerabil la modificări decât software. Dacă se folosesc algoritmi secreţi, aceştia trebuiesc implementaţi în cip-uri inviolabile. Implementările hardware pot include criptoprocesoare dedicate, generatoare de numere aleatoare şi/sau ceasuri foarte precise.

• **Siguranţa.** Un USC poate oferi siguranţa că un utilizator nu poate ocoli sau dezactiva mecanismele de custodie sau alte caracteristici. Un USC care poate fi folosit sau modificat pentru a "trişa", este numit un USC trişor (*Rogue*). Vom face distincţie între trişori simpli (*Simple Rogues*), care operează cu non-trişori şi trişori dubli (*Double Rogue*) care operează numai cu alţi trişori. Trişorii simpli prezintă ameninţarea cea mai mare pentru decriptarea forţată, deoarece nu necesită colaborarea destinatarului.

4. Componenta pentru custodia cheilor

KEC este responsabilă pentru memorarea tuturor cheilor necesare la recuperarea datelor prin decriptare forţată şi cu asistarea DRC-ului, prin furnizarea unor date sau servicii cerute.

• **Rolul în cadrul infrastructurii pentru gestiunea cheilor.** KEC poate fi parte componentă a infrastructurii pentru gestiunea cheilor (*Key Management Infrastructure*) care la rândul ei poate fi o infrastructură cu chei simetrice (*Single-Key Infrastructure*) sau cu chei publice (*Public-Key Infrastructure*). Ulterior, agenţii de custodie ar putea servi ca autorităţi pentru certificarea cheilor publice (*Public-Key Authorities*).

• **Agenţii de custodie.** Agenţii de custodie, numiţi şi părţi de încredere (*Trusted Parties*) sunt responsabili pentru operarea KEC-ului. Aceştia pot fi înregistraţi la un centru pentru custodia cheilor (*Key Escrow Center*), care coordonează activitatea lor sau serveşte ca punct de legătură între USC şi DRC. Agenţii de custodie sunt caracterizaţi de :

- *Tipul de agent.* Agenţii de custodie pot fi entităţi din sectorul guvernamental sau sectorul privat. Cei din prima categorie ar putea restricţiona serviciile lor numai pentru organizaţii guvernamentale. Cei din a doua categorie, care activează în cadrul sistemelor criptografice cu chei în custodie private sau comerciale, pot fi din interiorul unei organizaţii sau sub forma unor companii independente, oferind servicii comerciale sau de tip terţ de încredere.
- *Identificarea.* Aceasta include numele şi localizarea agentului.
- *Accesabilitatea.* Este determinată de localizarea agenţilor de custodie (locali sau străini) şi de orarul lor de funcţionare (24 ore pe zi, 7 zile pe săptămână).
- *Securitatea.* Aceasta se referă la cât de bine reuşeşte KEC să protejeze cheile aflate în custodie împotriva abuzului, compromiterii sau piederii lor.
- *Notificarea.* Aceasta asigură identificarea unui agent de custodie care sabotează recuperarea datelor sau care eliberează cheile unei persoane neautorizate sau în circumstanţe neautorizate.
- *Răspunderea.* Caracterizează modul în care agenţii de custodie sunt răspunzători de compromiterea sau nedisponibilitatea cheilor aflate în custodie.
- *Certificare / licenţiere.* Aceasta indică dacă agenţii de custodie sunt certificaţi sau licenţiaţi de agenţiile guvernamentale. Calificarea pentru obţinerea licenţei impune agenţilor de custodie să îndeplinească anumite condiţii specifice. Folosirea agenţilor de custodie licenţiaţi poate afecta exportabilitatea.

• **Cheile pentru recuperarea datelor.** Folosind criptografia cu chei în custodie, toate datele criptate sunt legate de cheile pentru recuperare, lucru ce permite accesul la cheile de criptare a datelor. Aceste chei pentru recuperare sunt caracterizate de :

- *Granulitatea cheilor.* Opţiunile pot fi:

Chei de criptare a datelor. Acestea pot fi chei de sesiune, chei de reţea şi chei de fişier. Un centru de distribuţie poate genera, păstra în custodie şi distribui asemenea chei.

Chei de produs. Acestea sunt unice pentru un USC.

Chei utilizator. În mod normal acestea sunt perechei de chei (publice-secrete) folosite pentru stabilirea cheilor de criptare. KEC poate servi ca autoritate de certificare a cheii

publice a utilizatorului, eliberând un certificat pentru cheia publică a utilizatorului.
Chei master. Aceste chei sunt asociate cu KEC şi sunt folosite de mai multe USC-uri.
- *Fragmentarea cheilor (partajarea secretului, scheme prag)*. O cheie pentru recuperarea datelor poate fi divizată în mai multe componente, fiecare componentă fiind deţinută de câte un agent de custodie. Cheile pot fi divizate astfel încât pentru refacerea cheii să fie necesari n agenţi sau oricare "k din n", unde k < n iar n reprezintă numărul agenţilor. Această divizare poate fi făcută folosind o structură de acces general monotonă ce permite specificarea submulţimilor arbitrare de agenţi care pot colabora pentru refacerea cheii.
- *Cine generează şi distribuie cheile*. Cheile pot fi generate de KEC sau USC sau o combinaţie a celor două componente. Dacă sunt generate de USC, cheile pot fi divizate şi date în custodie folosind scheme de partajare a secretului verificabile, astfel încât agenţii de custodie pot verifica componenta lor individuală fără a cunoaşte cheia originală. Cheile pot fi generate împreună, astfel ca un utilizator să nu poată ascunde o cheie "umbră", dintr-o cheie dată în custodie, ocolind astfel mecanismul de custodie.
- *Momentul de dare în custodie*. Cheile pot fi date în custodie pe timpul fabricării produ-sului, la iniţializarea produsului sau a sistemului sau la înregistrarea utilizatorului. Dacă se doreşte păstrarea în custodie a unei chei secrete a unui utilizator (dintr-o pereche de chei publice) ea poate fi dată în custodie atunci când cheia sa corespondentă publică intră în infrastructura de chei pubice şi s-a emis un certificat. Un USC poate trimite date criptate numai utilizatorilor cu certificate de chei publice semnate de agenţi de custodie aprobaţi.
- *Actualizarea cheilor*. Multe sisteme pot permite modificarea cheilor pentru recuperarea datelor. Aceste modificări se pot face la cerere sau la intervale regulate de timp.
- *Păstrarea cheilor*. Aceasta se poate face off-line (de exemplu pe dischete păstrate în seifuri sau smartcard-uri) sau on-line.

• **Servicii pentru recuperarea datelor**. KEC oferă servicii DRC-ului ce includ punerea la dispoziţie de informaţii pentru recuperare, caracterizate de :
- *Procedurile de autorizare*. Procedurile după care persoanele care operează sau folosesc DRC-ul accesează KEC, cuprind stabilirea dovezilor de identitate şi a autorităţii legale pentru accesul la datele ce se decriptează.
- *Servicii oferite*. Există mai multe opţiuni posibile:
Eliberearea cheilor pentru recuperarea datelor. Această variantă este folosită, în mod normal, când cheile pentru recuperarea datelor sunt chei de sesiune sau chei de utilizator sau produs (nu se eliberează cheile master). Cheile pot fi eliberate cu dată de expirare, după care acestea se distrug automat.
Eliberearea cheilor derivate. KEC eliberează chei derivate pentru recuperarea datelor cum ar fi chei dependente de timp, care permit decriptarea numai a datelor criptate de-a lungul unei perioade specificate de timp.
Decriptearea cheii. Această variantă este folosită când în DRC sunt folosite chei master pentru criptarea cheilor de sesiune (sau a cheilor utilizator); KEC nu trebuie să elibereze DRC-ului cheile master.
Decriptarea prag. Fiecare agent de custodie furnizează DRC-ului o "bucată" din decriptare; acesta combinându-le, obţine cheia de decriptare a textului.
- *Transmisia datelor* la şi de la DRC poate fi făcută fie manua, fie electronic.

• **Protecţia cheilor aflate în custodie**. KEC protejează cheile aflate în custodie împotriva compromiterii sau pierderii. Aceasta include o combinaţie de proceduri tehnice şi protecţii legale. Exemplele cuprind auditare, separare a responsabilităţilor, divizare a cunoştinţelor, control cu două persoane, securitate fizică, criptografie, redundanţă, testare şi validare independentă, certificare, acreditare precum şi legi ce prevăd sancţiuni pentru nerespectarea acestora.

5. Componenta de refacere a datelor

DRC ajută la refacerea datelor iniţiale din datele criptate, folosind informaţia furnizată

de KEC precum şi cea din DRF. Este caracterizat de :

• **Capabilităţi**. Acestea includ:

- *Decriptare în timp real a comunicaţiilor interceptate.*

- *Post-procesare*. DRC poate decripta comunicaţiile anterior interceptate şi înregistrate.

- *Transparenţă*. Decriptarea este posibilă fără ca părţile implicate să cunoască aceasta.

- *Independenţă*. Odată obţinute cheile, DRC poate decripta folosind resursele proprii, independent de KEC.

• **Refacerea cheilor de criptare**. Pentru a putea decripta, DRC trebuie să dobândească cheia de criptare K în următoarele moduri :

- *Accesul la expeditor sau destinatar*. Un factor critic este dacă K poate fi refăcută folosind datele asociate ale expeditorului sau ale destinatarului. Dacă accesul este posibil numai cu cheile deţinute de agentul de custodie al expeditorului, DRC-ul trebuie să obţină datele despre cheile în custodie pentru toate părţile ce transmit mesaje unui anumit utilizator, inclusiv în cazul în care părţile sunt în ţări diferite şi folosesc diferiţi agenţi de custodie. În mod asemănător, dacă accesul este posibil numai prin cheile deţinute de agentul de custodie al destinatarului, decriptarea în timp real a mesajelor transmise de un anumit utilizator ar putea fi imposibilă. Dacă refacerea datelor este posibilă folosind cheile deţinute de oricare agenţi de custodie, DRC poate decripta oportun comunicaţiile interceptate atât de la, cât şi pentru un anumit USC. Un sistem poate oferi această capabilitate pentru comunicaţii duplex (de exemplu convorbirile telefonice) cerând ca aceeaşi cheie K să fie folosită de ambele părţi.

- *Frecvenţa interacţionărilor cu KEC*. Poate fi nevoie ca DRC să interacţioneze cu KEC o dată pentru fiecare cheie de criptare sau o dată pentru fiecare USC sau utilizator. Prima variantă necesită o conexiune on-line între DRC şi KEC, pentru a suporta decriptarea în timp real a comunicaţiilor, când cheile de sesiune se modifică la fiecare conversaţie.

- *Necesitatea căutării exhaustive*. Dacă agentul de custodie returnează la DRC chei parţiale, acesta trebuie să folosească căutarea exhaustivă pentru determinarea biţilor rămaşi.

• **Protecţie la decriptare**. DRC poate folosi protecţii tehnice, procedurale şi legale pentru a determina ce poate fi decriptat. De exemplu, refacerea datelor poate fi restricţionată la o anumită perioadă de timp (autorizată de un mandat).

6. Câteva implementări notabile

Un domeniu important de utilizare a sistemelor cu chei în custodie este cel comercial, caz în care se permite decriptarea forţată a unor informaţii transmise prin reţea sau memorate în fişiere dacă se pierd cheile, dacă persoana responsabilă este absentă sau dacă se doreşte decriptarea unor fişiere de către servicii sau persoane autorizate din interiorul companiilor. Iată câteva dintre *realizările existente în domeniul utilizării comerciale a sistemelor cu chei în custodie.*

• **AT&T Crypto Backup,** este un proiect patentat pentru un sistem care realizează decriptarea de urgenţă a cheilor de cifrare a unor documente, cu ajutorul unei chei master păstrată în custodie.

• **Bankers Trust Secure Key Escrow Encryption System (SecureKEES).** Angajaţii unei corporaţii înregistrează dispozitivele lor de criptare (de exemplu smartcard-urile) şi cheile secrete de criptare la unul sau mai mulţi agenţi de custodie comerciali selectaţi de corporaţie.

• **Bell Atlantic Yaksha System** este un server on-line pentru securitatea cheilor; generează şi distribuie chei de sesiune şi chei de fişier, folosind a variantă a algoritmului RSA. Serverul transmite cheile părţilor autorizate pentru scopuri de refacere a datelor.

• **Blaze's Smartcard-Based Key Escrow File System** este un sistem criptografic cu chei în custodie bazat pe smartcard-uri, pentru lucru într-un sistem de cifrare a fişierelor. Utilizatorii dau în custodie cheia de criptare a unui fişier, pe un smartcard, unor agenţii de custodie.

• **The Clipper / Capstone Chips.** Aceste chip-uri implementează EES (Escrowed Encryption Standard) ce foloseşte algoritmul

secret Skipjack. Cheile unice pentru refacerea datelor programate pe fiecare chip sunt divizate între două agenţii guvernamentale şi restricţionate pentru uz guvernamental.

- **Cylink Key Escrow**. Această propunere foloseşte tehnicile Diffie-Hellman pentru integrarea serviciilor criptografice cu chei în custodie într-o infrastructură cu chei publice.
- **Fortezza Card**. Aceast card pentru PC conţine un chip Capstone. Cheile de criptare publice/secrete ale unui utilizator sunt memorate pe acest card şi sunt date în custodie la autoritatea de certificare a cheilor publice.
- **Kilian and Leighton Failsafe Key Escrow**. Cheile unui utilizator sunt generate de către utilizator împreună cu agenţii de custodie, astfel încât utilizatorul nu poate ocoli mecanismul de custodie.
- **Leiberich Time-Bounded with a Clock**. Această îmbunătăţirea a chip-ului Clipper oferă o refacere a datelor, cu ajutorul unor cheilor unice dependente de timp.
- **Lotus Notes International Edition (Differential Workfactor Cryptogrphy)**. Datele sunt criptate cu chei de 64 de biţi, dintre care 24 sunt criptaţi cu o cheie publică a unei organizaţii guvernamentale şi transmişi odată cu datele. Guvernul poate obţine ceilalţi 40 biţi rămaşi folosind căutarea exhaustivă.
- **Micali Fair Public Key Cryptosystems**. Propune tehnici de partajare a secretului verificabile în care utilizatorii generează, împart şi dau în custodie cheile lor private la agenţii de custodie doriţi, singura obligaţie fiind accea de a pune cheile lor publice în infrastructura de chei publice.
- **Nechvatal Public-Key Based Key Escrow System**. Această propunere foloseşte tehnicile cu chei publice Diffie-Hellman pentru custodia cheilor şi recuperea datelor.
- **Nortel Entrust**. Acest produs comercial arhivează cheile de criptare private ca parte a unei funcţii de autorizare a certificatelor şi a suportului infrastructurii cheilor publice.
- **Royal Holloway Trusted Third Party (TTP) Services**. Această arhitectură propusă pentru o infrastructură a cheilor publice necesită ca părţile terţi de încredere, împreună cu perechi de utilizatori care comunică, să partajeze chei şi paramêtri secreţi.
- **TIS Commercial Key Escrow**. Acesta este un sistem comercial de criptografie cu chei în custodie, folosit atât pentru memorarea datelor criptate cât şi pentru transfer de fişiere. Recuperarea datelor se face folosind chei master deţinute de un centru pentru recuperarea datelor.
- **TIS Software Key Escrow Paralleling Clipper**. Acest proiect propus este similar cu Clipper, numai că este implementat software şi nu hardware şi foloseşte criptografia cu chei publice pentru recuperarea datelor.

Ca răspuns la cererile reale de piaţă şi independent de eforturile guvernului, câteva companii au produs proiecte şi produse oferind custodia cheilor. Sistemele cu chei în custodie au şansa să devină utilizate larg în lume, deoarece el furnizează un serviciu util atât utilizatorilor individuali şi firmelor, cât şi autorităţilor statale.

Bibliografie

- Balenson, D. M., Ellison, C.M., Lipner, S.B., şi Walker, S.T. "*A new approach to software key escrow. TISR*", Trusted Information Systems, Glenwood, Md., 1994.
- Balenson, D. M. "*Wordwide availability of cryptographic products*", Trusted Information Systems, Glenwood, Md., 1995.
- Blaze, M. "*Protocol failure in the escrowed encryption standard*", The 2d ACM Conference on Computer and Communications Security, ACM Press, 1994.
- Denning D.E.,"*A Taxonomy for Key Escrow Encription Systems*", Comm.of ACM, 1996.
- Denning D.E.,"*Encryption Policy and Market Trends*", RSA Data Security Conference, 1997;
- Garfinkel S., Spafford G., "*Practical UNIX & Internet Securiy*", O'Reilly& Associates, 1996;
- RSA Data Security, Inc., "*The Keys to Privacy and Authentication*" , Products Catalog, Redwood City, USA, 1996;
- Schneier B., "*Applied Crypography*", John Wiley & Sons, 1996.
- The White House, "*Directive on public encryption management*", 1993