Identificació, autenticació i control d'accés

Antoni Martínez-Ballesté
Agustí Solanas
Jordi Castellà-Roca

PID_00177495

Universitat Oberta de Catalunya

Índex

Introducció

La proliferació dels sistemes informàtics ha ocasionat que la identitat dels usuaris s'hagi convertit en un factor clau estretament relacionat amb la seguretat. Ja en els primers sistemes, que només admetien que en fes ús un operador, s'havia de controlar l'accés a la màquina i les accions que es feien.

El desenvolupament de sistemes d'ordinador central (*mainframe*) amb molts terminals va possibilitar el treball multiusuari: cada usuari es pensava que disposava de la màquina íntegrament, quan en realitat els recursos eren repartits en temps i espai entre tots els usuaris. En aquell moment es va fer necessari el desenvolupament de sistemes d'identificació que en la mesura del possible estiguessin estretament lligats amb el sistema operatiu de l'ordinador central. Cada usuari s'havia d'identificar a la màquina mateixa per a fer ús dels recursos d'aquesta màquina. A més, la identificació va permetre monitorar qui usava cada recurs i en quin moment. Ara bé, qui ens assegurava que l'usuari connectat a l'ordinador era realment qui deia que era? L'autenticació és essencial perquè la identificació tingui sentit i sigui útil.

La universalització de serveis accessibles remotament basats en Internet ha fet créixer la importància de l'autenticació de la identitat. I encara és més important quan Internet és una plataforma que permet dur a terme accions que impliquen diners (comprar per Internet, presentar la declaració de la renda, etc.) o un control de la privadesa de l'usuari (xarxes socials, documents en el núvol, etc.). En aquest sentit, la signatura digital i les tecnologies que hi estan relacionades tenen un paper clau en l'autenticació segura.

En aquest mòdul estudiarem els diferents mètodes d'identificació i l'autenticació d'aquests mètodes, des de les clàssiques contrasenyes fins als certificats digitals, passant pels dispositius segurs d'identificació i apuntant el futur de la identificació per mitjà de la biometria. També donarem una visió de les tècniques de control d'accés i les metodologies d'implantació d'aquestes tècniques.

En el mòdul estudiarem les tècniques bàsiques d'autenticació i control d'accés. Sobre l'autenticació de la identitat dels usuaris, estudiarem en què consisteix l'autenticació i exposarem una panoràmica dels diferents tipus de mitjans que es poden utilitzar. També estudiarem conceptes relacionats amb el cicle de vida de la identitat digital, des de la creació fins a la baixa d'aquesta identitat, passant per detalls que s'han de tenir en compte a l'hora d'utilitzar les eines. El mòdul se centra, en general, en les tecnologies usades per a autenticació en

escenaris basats en Internet. Finalment, farem una panoràmica dels sistemes de control d'accés, estudiant les fases d'un sistema de control d'accés, les polítiques d'accés i els tipus de control d'accés.

Objectius

Els objectius que haurà assolit l'estudiant en acabar aquest mòdul són els següents:

1. Comprendre què és l'autenticació de la identitat.

2. Conèixer tècniques i conceptes relacionats amb les contrasenyes.

3. Comprendre el funcionament del certificat electrònic.

4. Conèixer els dispositius d'usuari que es poden utilitzar en l'autenticació.

5. Conèixer les tècniques que proporciona la biometria per a la identificació i l'autenticació.

6. Conèixer l'estructura del document nacional d'identitat electrònic.

7. Comprendre els passos necessaris per a donar d'alta usuaris d'un servei telemàtic.

8. Comprendre els mecanismes d'autenticació en un servei telemàtic.

9. Conèixer el procediment de la baixa d'usuaris d'un servei telemàtic.

10. Comprendre què és el control d'accés.

11. Conèixer les fases i polítiques del control d'accés.

12. Comprendre el funcionament dels principals tipus de control d'accés.

1. Tècniques d'identificació i autenticació

Inici de sessió

Per a fer referència a l'identificador d'usuari s'utilitza el terme *inici de sessió* o *login*.

La identificació digital forma part indissoluble de la majoria de serveis a Internet i les tecnologies de la informació i la comunicació (TIC). Per exemple, per a penjar un vídeo en un servidor, es demana que l'usuari estigui donat d'alta en el servei i s'identifiqui per a dur a terme la publicació del contingut. D'altra banda, per a utilitzar una xarxa social, cal que l'usuari estigui registrat. Així mateix, els contactes d'aquesta xarxa també han d'estar identificats convenientment. Per a dur a terme accions tan variades com fer un pagament amb targeta de crèdit, utilitzem aquesta mateixa targeta per a identificar-nos. O bé per a dur a terme gestions bancàries per Internet, el primer que hem de fer és especificar qui som.

Aquesta identificació digital pot ser relativament senzilla. N'hi ha prou de tenir un nom d'usuari, usar com a identificador l'adreça de correu electrònic o, en el cas d'un pagament, usar el número de la targeta de crèdit. Ara bé, per a la majoria de serveis, a més de la identificació digital, cal una autenticació d'aquesta identitat.

Mitjançant l'autenticació de la identitat, el servei s'assegura que l'usuari és qui diu que és.

La qüestió de "qui diu que és" la resol l'identificador d'usuari: mitjançant una cadena de caràcters es denota quina és la identitat de l'usuari. I per a demostrar l'autenticitat de la identitat de l'usuari es poden usar quatre acostaments diferents:

1) L'usuari és qui diu que és si demostra que sap alguna cosa que solament ell pot saber. Per exemple, si sap una paraula secreta d'accés.

2) L'usuari és qui diu que és si té algun objecte, com per exemple una targeta magnètica. Un exemple no relacionat amb la informàtica són les claus de casa: en principi, és el propietari qui les té.

3) L'usuari és qui diu que és si té alguna característica física que només té ell; per exemple, l'empremta dactilar.

4) L'usuari és qui diu que és si és capaç de fer una cosa de manera única; per exemple, el patró d'escriptura o la manera de caminar.

Malgrat que es tracta de quatre maneres d'abordar l'autenticació de la identitat, no hi ha una frontera clara entre algunes d'aquestes maneres. A més, és ben possible l'ús de diverses d'aquestes tècniques de manera combinada, per a aconseguir graus de seguretat més alts.

Per exemple, el fet de tenir una targeta amb codis de seguretat per a permetre operacions bancàries per Internet (targeta de coordenades) es podria veure com una barreja entre els dos primers casos: l'usuari té la targeta, però es pot dir que és coneixedor d'una informació, encara que en aquest cas la tingui escrita.

D'altra banda, totes aquestes maneres d'abordar l'autenticació no estan exemptes de problemes de seguretat. Per exemple, la targeta amb codis podria ser robada i usada per un altre usuari. Un altre cas és l'obtenció d'una clau d'accés mitjançant un correu electrònic fraudulent.

La usurpació d'identitat consisteix en el fet que una entitat usi amb èxit el mecanisme d'identificació que identifica una altra identitat.

En aquest apartat exposem les tècniques i les tecnologies per a implantar la identificació i autenticació d'usuaris.

1.1. Contrasenyes

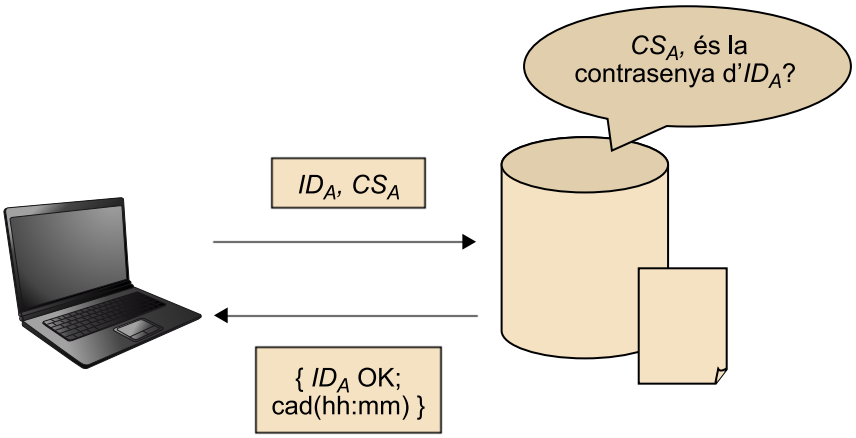
L'autenticació per mitjà de contrasenyes és relativament senzilla: l'usuari A envia el seu identificador ID_A i tot seguit la seva contrasenya CS_A. La implementació del protocol d'identificació pot precisar que totes dues informacions s'enviïn en un mateix missatge, o bé que primer es demani el nom d'usuari i després la contrasenya.

Aquesta contrasenya és usada pel servei per a validar la identitat de l'usuari. Si A és l'únic coneixedor de CS_A, és molt probable que l'usuari sigui realment A. En la figura, l'usuari utilitza la seva contrasenya per a validar-se en el servei, que té una llista de parelles d'usuaris i contrasenyes per a comprovar les identitats. Davant una contrasenya correcta, el servei envia un missatge d'autenticació correcta a l'equip de l'usuari. Fixem-nos que aquest missatge inclou una hora de caducitat d'aquesta autenticació, després de la qual l'usuari s'ha de tornar a autenticar.

Vegeu també

En l'apartat 2 estudiarem variants en l'ús de les contrasenyes, diferents formes d'emmagatzematge i gestió, i també algunes polítiques de seguretat.

Esquema de funcionament d'autenticació amb contrasenya



La contrasenya és una cadena de caràcters de longitud arbitrària. En alguns escenaris, s'usa una versió reduïda de la contrasenya, formada tan sols per uns quants nombres. En aquest cas la contrasenya es coneix amb el nom de *PIN*[1]. De totes maneres, en alguns entorns s'utilitza el terme *PIN* quan en realitat la contrasenya està formada tant per lletres com per nombres.

(1)*PIN* són les sigles de *número d'identificació personal* o *personal identification number*.

Així com un mateix servei o sistema no permet que hi hagi dos usuaris amb el mateix identificador, és ben possible que dos o més usuaris tinguin la mateixa contrasenya.

1.2. Certificats electrònics

Els sistemes de **criptografia de clau pública** representen una altra forma d'autenticació davant un servei. La signatura electrònica o els certificats electrònics són dues de les utilitats que serveixen per a fer l'autenticació d'identitat. A continuació, revisem alguns conceptes bàsics sobre criptografia de clau pública.

1.2.1. Sistemes de clau pública

Els sistemes de criptografia de clau pública (o asimètrics) es basen en l'ús de dues claus: la **clau privada** o secreta, que només sap el propietari, i la **clau pública**, la qual, com indica el nom, la poden saber altres entitats sense que això tingui conseqüències en la seguretat del sistema. En canvi, la clau privada ha d'estar ben custodiada. Els matemàtics, criptògrafs i organismes han proposat sistemes i estàndards de sistemes de clau pública. Aquests criptosistemes estan basats en funcions matemàtiques amb parany, que permeten fer una operació en un sentit fàcilment, però la inversa d'aquesta operació no és possible calcular-la computacionalment sense una informació extra (trapa). És a dir, amb la clau pública es fa una operació que únicament es pot invertir amb la clau privada, i viceversa.

Protecció de les claus privades

Les claus privades es guarden protegides en el programari amb una contrasenya, o bé en un dispositiu segur com una targeta intel·ligent (al qual també s'accedeix amb una contrasenya).

Vegeu també

El concepte de *targeta intel·ligent* l'estudiarem en el subapartat 1.3 d'aquest mòdul mateix.

L'ús de la clau pública o la clau privada depèn de l'operació que s'ha de fer:

- Per a donar **confidencialitat** a un missatge que *A* (emissor) envia a *B* (receptor), és a dir, per a fer que cap altre usuari no pugui saber el contingut del missatge, *A* ha d'usar la clau pública de *B* (que pot obtenir qualsevol usuari). Quan *B* rebi el missatge, ha d'usar la seva corresponent clau privada per a accedir al contingut del missatge. És recomanable que la clau privada estigui protegida i s'hagi de proporcionar una contrasenya per a accedir-hi.

- Per a donar **autenticitat** a un missatge que *A* envia a *B*, cosa que es coneix com a *signatura electrònica*, *A* usa la seva clau privada per a signar el missatge, operació que solament pot fer el posseïdor de la clau privada. Quan *B* rebi el missatge ha de comprovar la validesa de la signatura. Primer ha d'obtenir la clau pública de *A*, i a continuació ha de fer l'operació inversa a la signatura (verificació).

La signatura electrònica permet aconseguir tres propietats relacionades amb la seguretat de la informació. Amb la signatura electrònica d'un missatge (o fitxer) *M* enviat de *A* a *B*:

1) S'assegura que ningú no ha modificat el missatge signat. S'assegura, doncs, la **integritat** del missatge. La modificació d'un únic bit de la signatura o del missatge signat dóna lloc a una verificació incorrecta.

2) S'assegura que el missatge l'ha signat *A*, és a dir, s'assegura la **identitat** del signatari (o **autenticació d'origen** de *M*). L'operació únicament la pot fer el propietari de la clau privada.

3) Davant qualsevol tercera part, com que *A* és l'únic que sap la seva clau privada, es podrà demostrar que va ser *A* qui va signar *M*. O dit al revés, *A* **no podrà repudiar** la signatura electrònica feta del missatge. Únicament *A* pot fer aquesta operació (signatura).

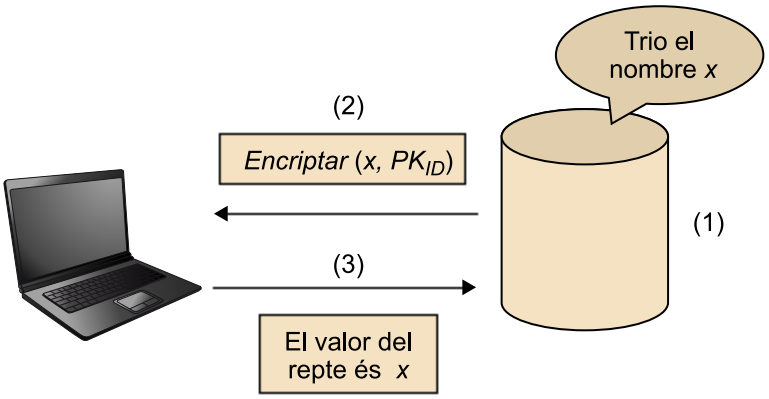
El fet de no compartir una clau entre qui encripta i qui desencripta, cosa que ocorre en els sistemes de clau compartida (o simètrics), proporciona aquestes dues últimes característiques de seguretat. Així, doncs, els sistemes de clau compartida no garanteixen completament la identitat i el no-repudi.

La signatura electrònica garanteix les propietats d'integritat, identitat i no-repudi.

La criptografia de clau pública permet un senzill sistema d'autenticació: el **sistema repte-resposta**. El servei obté la clau pública de la identitat que s'autentica (PK_{ID}). Llavors, el servei tria un nombre a l'atzar, l'encripta amb PK_{ID}

i envia aquest repte a la identitat. Si la identitat és qui diu que és, ha de tenir accés a la clau privada amb què ha de desencriptar el repte, de manera que ha de poder enviar de tornada el nombre aleatori amb què l'ha reptat el servei.

Esquema del sistema d'autenticació repte-resposta



Altres formes de repte-resposta

També es pot fer un repte-resposta amb una clau secreta compartida. Aquest cas és habitual amb l'ús de testimonis o *tokens*, que estudiarem més endavant.

L'ús de la signatura electrònica i en general dels sistemes de clau pública planteja dos grans problemes, que tractarem a continuació. D'una banda, quan s'obté la clau pública d'una entitat (correu electrònic, servidor d'Internet, etc.), com s'assegura que correspon realment a l'entitat identificada? D'altra banda, en vista que cada dia hi ha més processos comercials, administratius, fiscals, etc. que es poden fer telemàticament, quina empara legal tenen els sistemes de signatura electrònica?

1.2.2. Autenticitat de la clau pública

El fet d'assegurar que una clau pública correspon a una entitat es duu a terme amb un **certificat electrònic**.

L'objectiu d'un certificat electrònic (o digital) és donar fe de la vinculació d'una clau pública a una identitat, com un usuari o un servei.

Exemples de certificat electrònic

Quan ens connectem a un lloc web segur s'obté un certificat la missió del qual és autenticar la identitat del servidor. D'altra banda, quan fem una signatura electrònica en un document, aquesta signatura s'acompanya, en general, d'un certificat que dóna fe de la validesa de la clau pública que s'ha d'usar per a comprovar la signatura.

La informació bàsica que conté un certificat és la següent:

- La identitat que se certifica; per exemple, una adreça de correu electrònic o el número del document nacional d'identitat (DNI) d'un ciutadà.
- El període de validesa, que és la data a partir de la qual el certificat no serà reconegut com a vàlid.
- La clau pública que se certifica, que s'usarà directament per a comprovar la signatura.
- El nom de l'emissor del certificat. En general, es tracta d'una **autoritat de certificació**, un organisme que pot expedir certificats de clau pública.

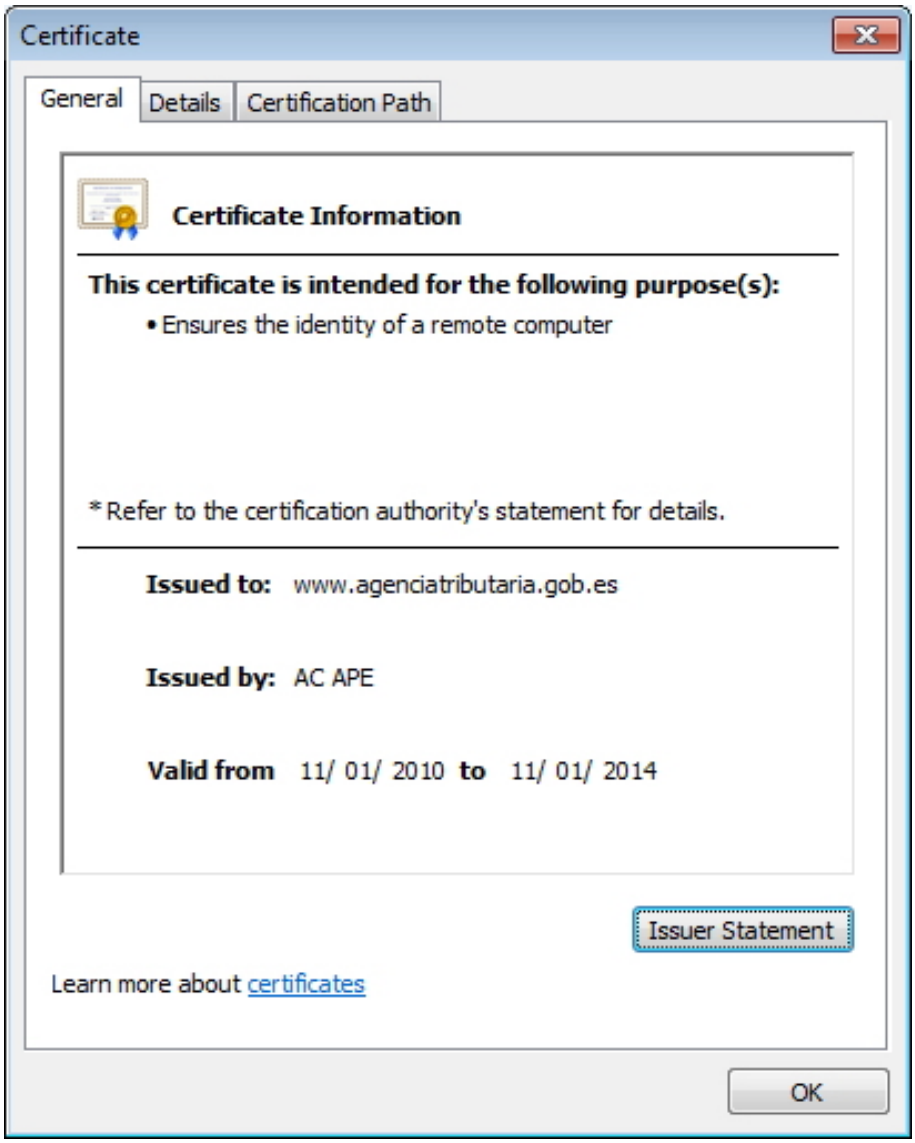
Aquesta autoritat dóna fe que la clau pública pertany a la identitat especificada en el certificat.

Les autoritats de certificació disposen d'una plataforma telemàtica (infraestructura de clau pública, PKI) que permet generar i gestionar claus i certificats.

Aquest últim element és crucial per al funcionament dels sistemes de clau pública. Hem vist que una clau pública està autenticada amb un certificat. Per a confiar en un certificat, doncs, s'ha de confiar en l'emissor d'aquest certificat. Això és, si l'emissor no és de confiança, el certificat s'ha de rebutjar. Si, per contra, l'emissor és de confiança, el certificat és acceptat i, en conseqüència, es dóna per bona la clau pública que certifica.

La figura mostra les propietats del certificat de servidor de la Seu Electrònica de l'Agència Tributària. L'objectiu és assegurar la identitat del servidor www.agenciatributaria.gob.es. S'hi observa el període de validesa que té i qui emet el certificat (Agència de Certificació de l'Administració Pública Espanyola, ACAPE).

Certificat de l'Agència Tributària per als seus serveis web



Ara bé, la discussió pot ser què vol dir confiar en un emissor. Un sistema informàtic d'usuari (ordinador, navegador, etc.) disposa, per defecte, d'unes entitats emissores de certificats de confiança. En aquest sentit, els sistemes tenen un magatzem de certificats en el qual hi ha una col·lecció d'entitats de confiança. Si es rep un certificat que ha estat emès per una autoritat de confiança, s'accepta aquest certificat sense més ni més (de fet, l'usuari no és ni conscient d'aquest fet). La dificultat sorgeix quan l'emissor del certificat no és a la llista d'autoritats de confiança del sistema. En aquest cas, se sol mostrar un missatge d'informació i és l'usuari qui ha de decidir si accepta l'emissor del certificat rebut com una nova autoritat de confiança (a partir de llavors, els futurs certificats que es rebin i hagin estat emesos per aquesta autoritat seran acceptats com a vàlids, sense preguntar a l'usuari).

Les grans empreses certificadores internacionals, i també organismes certificadors dependents dels governs, ja són reconegudes per la majoria del programari criptogràfic.

1.2.3. Legalitat de la signatura electrònica

Per a fer aplicacions que permetin una signatura electrònica a la Unió Europea, s'ha de tenir present la legislació pertinent, amb la qual es pugui saber amb quines signatures s'ha de treballar, quines característiques fan legal una signatura en un determinat moment i quines dades s'han de verificar.

Els països de la Unió Europea es regeixen per la Directiva 1999/93/CE, de 13 desembre, per la qual s'estableix un marc comunitari per a la signatura electrònica. Posteriorment, cada país membre fa la transposició de la Directiva dins de la seva legislació de la manera que considera més convenient.

En particular, dins de la legislació espanyola, es regula la signatura electrònica en la Llei 59/2003, de 19 de desembre, de signatura electrònica, la qual defineix dos tipus de signatura electrònica en l'article tercer, "Signatura electrònica i documents signats electrònicament", del títol I, "Disposicions generals":

1) La **signatura electrònica** és el conjunt de dades en forma electrònica, consignades o associades amb d'altres, que poden ser utilitzades com a mitjà d'identificació del signatari. Per exemple, un PIN o una signatura electrònica. Aquest tipus de signatura no té efectes jurídics totals. No és prou segura, ja que no es garanteix que hagi estat creada pel suposat signatari; es pot tractar d'una signatura reproduïble per un usuari malintencionat.

2) La **signatura electrònica avançada** permet identificar el signatari i detectar qualsevol canvi ulterior de les dades signades; està vinculada al signatari de manera única i a les dades a què es refereix, i és creada per mitjans que el signant pot mantenir sota el seu control exclusiu. Pot ser considerada no prou segura si el seu algorisme és feble o si hi ha hagut un compromís de la clau privada –de manera que la signatura no l'hauria feta el signant–, o si pot ser reproduïble (és a dir, si s'hi poden fer atacs per força bruta per a crear signatures). Un tipus específic de signatura electrònica avançada és la reconeguda.

Una **signatura electrònica reconeguda** és una signatura electrònica avançada basada en un certificat reconegut i generada amb un dispositiu segur de creació de signatura. S'equipara completament a la signatura manuscrita.

Nota

El DNI electrònic permet una signatura electrònica reconeguda.

Cal esmentar també la Decisió de la Comissió de 14 de juliol del 2003, relativa a la publicació dels números de referència de les normes que tenen reconeixement general per a productes de signatura electrònica.

Els diferents tipus de signatura electrònica estan definits, dins de la Unió Europea, segons la Norma ETSI TS 101 733 CMS *Advanced Electronic Signatures* (CAdES), o l'equivalent que té en XML, és a dir, ETSI TS 101 903 XML *Advanced Electronic Signatures* (XAdES):

- **Signatura electrònica bàsica**.
- **Signatura electrònica avançada**. La implantació es fa com a ASN.1/CMS o S/MIME, o XML-Dsig.
- **Signatura electrònica amb marcatge de temps** o *timestamping*. S'incorpora a la signatura la data en què es duu a terme.
- **Signatura electrònica completa**. Inclou dades de verificació. Equival a la signatura electrònica reconeguda dins de la legislació espanyola.
- **Signatura electrònica estesa**. Inclou dades de verificació amb marcatge de temps.

Organitzacions d'estandardització

Les organitzacions encarregades de l'estandardització dels formats de signatura electrònica i recomanacions són l'European Telecommunications Standards Institute (ETSI), que és l'encarregada oficial dins de la Unió Europea, la Internet Engineering Task Force (IETF), a escala internacional, i el World Wide Web Consortium (W3C), també a escala internacional.

Els estàndards més comuns en signatura electrònica són els següents:

- PKCS#7 (*Public Key Cryptographic Standard*). Definit en l'RFC 2315.
- IETF RFC 2630 / RFC 3369 (*Cryptographic Message Syntax*, CMS). Sintaxi ASN.1. Basada en PKCS#7.
- ETSI TS101733. CAdES. Estàndard europeu basat en CMS per a signatures ASN.1.
- Estàndards de signatura basats en XML més comuns:
  - Signatura XML, XML-Dsig, Dsig XML o XML-Sig. Recomanació del W3C, que defineix una sintaxi XML per a la signatura electrònica. Basada en PKCS#7. S'utilitza en tecnologies web com SAML. Defineix un format per a transportar signatures electròniques.
  - XAdES: extensió d'XML-Dsig definida per l'ETSI TS101903. És l'estàndard europeu basat en XML-Dsig per a signatures XML.

Signatura de documents ofimàtics i PDF

Els documents PDF (format de document portàtil o *portable document format*) poden ser signats electrònicament, igual que altres formats de document ofimàtic. Utilitzen estructures pròpies per a guardar la informació de la signatura.

1.2.4. Signatures XML

La facilitat que dóna XML per a estructurar la informació, el fet de ser lliure de llicències i la independència que té de la plataforma repercuteixen en el fet que aquesta tecnologia sigui una de les més esteses per a signar documents generats al Web. L'estàndard de referència és XML (signatura electrònica avançada

o *advanced electronic signature*), més conegut per l'acrònim *XAdES*, segons la Directiva europea per a signatura electrònica, per la qual cosa defineix formats de signatura que puguin ser vàlids per a fer transaccions.

Hi ha diversos tipus de XAdES que implementen una XML-Dsig, segons el nivell de protecció ofert. A continuació es defineixen alguns dels nivells de protecció de XAdES, del més bàsic al més extens, cadascun dels quals inclou i estén el previ:

- **XAdES-BES** (*basic electronic signature*). Defineix la forma bàsica d'una signatura electrònica. Ha de contenir l'element *SigningCertificate* o *ds:KeyInfo*.

- **XAdES-EPES** (*explicit policy based electronic signature*). Afegeix informació sobre polítiques de signatura mitjançant la propietat *SignaturePolicyIdentifier*.

- **XAdES-T**. Afegeix un camp de marcatge de temps mitjançant *SignatureTimeStamp* o d'un proveïdor de temps de confiança.

- **XAdES-C**. Afegeix referències a dades de verificació (certificats i llistes de revocació) als documents signats per permetre la verificació i validació fora de línia o *off-line*.

- **XAdES-X**. Signatura estesa amb marques de temps a les referències introduïdes per XAdES-C per a evitar que quedi compromesa en el futur una cadena de certificats, mitjançant les propietats *CompleteCertificateRefs* i *CompleteRevocationRefs*.

- **XAdES-X-L**. Signatura estesa a llarg termini afegint els certificats i les llistes de revocació als documents signats, per a permetre la verificació en el futur fins i tot si les fonts originals (de consulta de certificats o de les llistes de revocació) ja no estan disponibles per mitjà de les propietats *CertificateValues* i *RevocationValues*.

- **XAdES-A**. Signatura arxivada que afegeix la possibilitat de marcatge de temps periòdic de documents arxivats per mitjà de les propietats *CertificateValues*, *RevcationValues* i almenys un *ArchivedTimeStamp*. Aquesta signatura prevé que la signatura del document pugui ser compromesa posteriorment a causa de la debilitat de la signatura.

Vegeu també

En el subapartat 2.3.2 d'aquest mòdul estudiarem en què consisteixen les llistes de revocació.

El W3C és l'encarregat de fer les recomanacions i definir la sintaxi XML per a gestionar signatures electròniques, i permetre així que una signatura XML pugui signar qualsevol tipus de document.

Hi ha diversos tipus de signatura XML, entre els quals remarquem els tres més comuns:

- ***Enveloping signatures***[2]. La signatura engloba el contingut que es troba dins d'un element Object de la mateixa signatura. L'objecte (o el contingut d'aquest objecte) és identificat mitjançant una referència (amb un identificador de fragment URI o transformació).

(2)En català, *signatura envolupant*.

- ***Enveloped signatures***[3]. La signatura engloba el contingut XML que conté la signatura com un element. El contingut proporciona l'element arrel del document XML. Òbviament, les signatures embolicades han d'anar amb compte de no incloure el seu propi valor en el càlcul de la *SignatureValue*.

(3)En català, *signatura embolicada*.

- ***Detached signatures***[4]. Aquesta signatura pot ser de dues formes: sobre un document extern o sobre part del document.

(4)En català, *signatura separada*.

Estructura bàsica de l'element `<Signature>`

```
<Signature ID?>
   <SignedInfo>
   <CanonicalizationMethod />
   <SignatureMethod />
   (<Reference URI? >
   <Transforms>)?
   <DigestMethod>
   <DigestValue>
   </Reference>)+
   </SignedInfo>
   <SignatureValue />
   (<KeyInfo />)?
   (<Object ID?>)*
</Signature>
```

Per a implementar la signatura d'un document amb XML, s'ha de tenir en compte que les representacions de documents signats usats per l'aplicació que fa la signatura i la que la verifica han de ser completament idèntiques. De fet, és completament possible que dues aplicacions diferents obtinguin, cadascuna, un document diferent de l'altre, però vàlids tots dos, a causa potser de la pertorbació de l'ordre dels atributs, dels possibles espais en blanc en les etiquetes, dels elements buits, etc. Per a assegurar que no hi hagi cap problema, el W3C defineix una **forma canònica** per a qualsevol document XML, i elimina així possibles ambigüitats en la generació de la representació d'un document. L'element `<SignedInfo>` i el document XML han de passar per aquest procés. Amb la canonització, ens assegurem que el document està codificat en UTF-8, no hi ha salts de línia, hi ha tots els atributs per defecte de cada element, etc.

1.3. Dispositius d'usuari

Fins ara, la gran majoria de serveis d'Internet usen la contrasenya com a eina d'autenticació. Les xarxes socials o els serveis de correu electrònic més populars en són alguns exemples. Els certificats digitals són usats generalment per a autenticar serveis que requereixen un nivell de seguretat elevat, com per exemple el lloc web segur d'un servei bancari en línia. No obstant això, en alguns serveis que funcionen sobre Internet ja és habitual que l'autenticació de la identitat sigui amb un certificat de client.

En general, per a usar aquest sistema d'autenticació, s'acaba usant una clau privada que hi ha en el sistema mateix o en un dispositiu extern. Aquesta clau secreta ha d'estar protegida (encriptada), i només s'ha de poder usar després d'introduir una contrasenya o PIN. De vegades, la mateixa contrasenya introduïda per l'usuari s'usa com a clau per a desencriptar la clau secreta i poder-la usar.

En general, doncs, els certificats i les claus secretes estan guardats en un equip de treball. De totes maneres, en determinats àmbits, és més còmode o fins i tot necessari disposar d'un dispositiu extraïble que sigui el que protegeixi aquesta informació.

Els testimonis de seguretat són petits dispositius l'objectiu dels quals és donar suport al procés d'autenticació d'identitat. En general s'utilitzen per a validar l'entrada a sistemes i serveis.

Hi ha gran varietat de testimonis. Per exemple, pel que fa a connexió a l'equip, els més habituals són els que es connecten al port USB, encara que també n'hi ha que usen una connexió Bluetooth o simplement no necessiten connexió a l'equip. Pel que fa a capacitat de memòria i procés, depèn del sistema de suport amb què funcioni el testimoni. Heus aquí quatre casos que combinen les alternatives anteriors:

Exemple d'ús de testimonis

Hi ha sistemes d'autenticació que usen testimonis entesos com a fitxers amb els quals els usuaris poden accedir als serveis. Un exemple d'això és el sistema Kerberos, amb el qual els usuaris obtenen, de manera transparent, fitxers amb què s'autenticaran davant serveis.

- El testimoni guarda un valor secret a la seva memòria i es comunica mitjançant USB amb un controlador instal·lat al PC. El controlador només permet l'accés al contingut del testimoni després de posar un PIN correcte. En el fons, la informació que conté la memòria està encriptada, i cal que el controlador la desxifri.

- El testimoni no està connectat a l'ordinador però té un petit teclat numèric amb el qual l'usuari introdueix una coordenada proporcionada pel sistema d'identificació. El testimoni mostra en una pantalla petita el valor secret corresponent a la coordenada sol·licitada. Aquest exemple és anàleg a la targeta de coordenades comentada més amunt.

- Un tercer cas és un testimoni amb capacitats criptogràfiques que pugui respondre a un repte criptogràfic enviat pel sistema d'identificació, usant el mètode repte-resposta. En aquest cas, es preveu la modalitat de repte-resposta usant una clau secreta compartida o bé usant un sistema d'encriptació de clau: la còpia de la clau secreta que necessita el client està emmagatzemada en el testimoni.

- Un últim cas és el d'una etiqueta RFID[5] que conté un valor que permet identificar l'etiqueta. Com que un lector d'RFID interactua amb les etiquetes mitjançant l'espectre electromagnètic i sense usar connexions físiques, el fet que la identificació sigui segura (que bàsicament estigui protegida contra escoltes d'atacants) comporta un repte important inherent a l'ús d'aquestes etiquetes en serveis i entorns que necessitin certa seguretat.

(5)*RFID* és l'abreviació d'*identificació per radiofreqüència* o *radiofrequence identification*.

Seguretat de les etiquetes RFID

El reduït rang de lectura fixat en els dispositius RFID dificulta l'atac, encara que no l'elimina per complet. Un atacant es pot acostar a la víctima per ser dins del rang de lectura de l'RFID i a continuació enviar aquesta informació mitjançant una connexió d'alta velocitat al sistema informàtic per autenticar-se. Per aquest motiu, cal fixar mesures de seguretat que requereixin la participació del propietari en l'autenticació.

Sigui com sigui, el testimoni és un dispositiu independent de l'ordinador i es pot portar sempre a sobre. Això implica un clar problema de seguretat en cas de robatori del testimoni.

Exemples de dispositius testimoni. A l'esquerra, testimoni sense contacte; a la dreta, testimoni USB. Font: Viquipèdia

Un altre element que es pot considerar testimoni és la targeta intel·ligent. Aquest tipus de targetes es caracteritzen pel fet de portar un circuit integrat capaç d'emmagatzemar informació i fins i tot fer operacions criptogràfiques. L'ús d'aquestes targetes es va popularitzar gràcies a l'acceptació que van tenir com a mitjà de pagament (comporten un nivell avançat en seguretat respecte de les targetes bancàries amb banda magnètica, ja que per a usar-les s'ha de saber un PIN), i també per les targetes mòdul d'identificació de l'abonat o *subscriber identity module* (SIM), que tenen actualment tots els telèfons mòbils. A més, en moltes organitzacions i institucions l'ús dels certificats digitals i les targetes intel·ligents s'ha convertit en una cosa habitual.

Claus d'un certificat digital

L'elevat ús d'operacions criptogràfiques afebleix la seguretat del parell de claus que componen un certificat digital. Creant dos parells de claus privades i públiques, s'aconsegueix reduir les possibilitats de debilitament de les claus. Un dels parells de claus s'utilitza per a les operacions d'autenticació, i l'altre, per a les de signatura de documents.

Seguretat de les targetes intel·ligents

En anglès, una targeta intel·ligent es diu *smart card* i, en francès, *carte à puce* ('targeta amb xip'). Les targetes intel·ligents són segures contra manipulacions. Si un atacant intenta accedir a la informació que conté, es bloqueja la targeta i s'elimina la informació. A més, incorporen mecanismes de protecció per a evitar que es pugui obtenir informació de les claus a partir del consum d'energia o temps de resposta.

Un altre ús que ha contribuït a la generalització del certificat digital és que sigui la plataforma del document nacional d'identitat electrònic (DNIe).

1.3.1. El document nacional d'identitat electrònic

El DNIe és una targeta intel·ligent capaç de guardar de manera segura informació i de processar-la internament. Aquesta propietat permet les accions següents:

- Acreditar electrònicament i de manera segura la identitat de la persona.
- Signar digitalment documents electrònics, i atorgar-hi així una validesa jurídica equivalent a la que hi proporciona la signatura manuscrita.

La targeta de suport del DNIe conté les dades de filiació del ciutadà, les dades biomètriques (model dactilar, foto i signatura manuscrita) i els dos parells de claus RSA amb els certificats digitals respectius, un d'autenticació i un altre de signatura electrònica.

Per a usar el DNIe, igual que amb altres targetes intel·ligents, cal un lector de targetes, com per exemple el que mostra la figura:

Imatge d'un lector de targetes intel·ligents amb un DNIe introduït

Protecció del DNIe

El DNIe manté el material criptogràfic sensible sempre a dins seu i en protegeix l'ús gràcies a un control d'accés amb un número d'identificació personal que només sap l'usuari.

La informació en el xip està distribuïda en tres zones amb diferents nivells de seguretat i condicions d'accés:

- **Zona pública**. La lectura d'aquesta zona és accessible sense restriccions. Conté, entre altres coses, el certificat de l'emissor i unes claus per a encriptar l'intercanvi d'informació entre el xip i el dispositiu de lectura. Aquestes claus estan certificades amb un certificat de component.

- **Zona privada**. La lectura d'aquesta zona està permesa al ciutadà, mitjançant el número d'identificació personal o PIN. Conté un **certificat d'autenticació** (que té com a finalitat garantir electrònicament la identitat del ciutadà en fer una transacció telemàtica) i un **certificat de signatura**. Aquest últim certificat és el que s'utilitza per a la signatura de documents, de manera que garanteix la integritat del document i el no-repudi. Aquest certificat expedit com a certificat reconegut i creat en un dispositiu segur de creació de signatura és el que converteix la signatura electrònica avançada en signatura electrònica reconeguda, i permet així que s'equipari legalment amb la signatura manuscrita.

- **Zona de seguretat**. Els ciutadans poden accedir a aquesta zona en els punts d'actualització del DNIe. Conté les dades impreses en el suport físic del DNI, la fotografia i la signatura escanejada.

Certificat de component

El certificat de component permet l'autenticació mútua de dispositius tal com es descriu en l'estàndard CWA-14890.

Encara que l'Administració pública ofereix molts tràmits en línia, la realitat és que la gran majoria de ciutadans que tenen DNI (gairebé tots en versió electrònica) encara no són coneixedors de les utilitats que té o bé no tenen els coneixements tècnics adequats per a usar-lo.

1.4. Biometria

La biometria significa si fa no fa una cosa com "mesurar" els trets "biològics" d'un individu.

> La biometria és l'aplicació de les matemàtiques i la ciència de la computació per a identificar individus d'acord amb els seus trets o característiques físics.

Aquesta tecnologia fa anys que apareix com a sistema d'autenticació habitual en la literatura i les pel·lícules de fantasia i ciència-ficció. De totes maneres, l'anàlisi de l'iris, la forma de la mà, fins i tot la manera de caminar, etc., ja tenen un paper important en sistemes de control d'accés reals. A més, és sabut que l'ús de les empremtes dactilars per a la identificació d'un individu ja és un sistema clàssic en organismes policials.

En un sistema biomètric, l'individu, abans que res, s'ha de registrar. Llavors un sistema d'informació registra una o més característiques físiques o de conducta. Per a identificar-lo, el sistema d'informació recull les característiques de l'individu que es vol identificar per fer una comprovació a la base de dades. Si la informació recollida no coincideix amb cap dels individus registrats, li és denegat l'accés.

Si el nombre d'individus registrats és molt elevat, el sistema no busca entre tots els individus de la base de dades, ja que pot arribar a ser costós i potenciador d'errors. L'individu que es vol identificar ho fa amb un codi (o qualsevol altre identificador), mentre que el sistema biomètric comprova que les característiques físiques recollides per a l'individu amb l'identificador concret coincideixen amb les emmagatzemades. En aquest cas, el sistema biomètric fa una autenticació de la identificació.

No obstant això, hi ha diferents problemes a què s'ha de fer front. En primer lloc, la recollida de característiques: els sistemes han d'obviar sorolls, imperfeccions o diferents matisos que els sistemes captadors i sensors recullen en cada accés d'un individu. En segon lloc, s'han de minimitzar les taxes d'errors del sistema d'identificació: no s'ha de permetre l'autenticació d'un individu no registrat o no vàlid i, al contrari, no s'ha de denegar l'autenticació correcta d'un individu registrat o vàlid. En aquest sentit, la taxa de fals positiu[6] i la de fals negatiu[7] mesura el bon funcionament i rendiment del sistema biomètric.

(6)En anglès, *false acceptance rate.*

(7)En anglès, *false nonmatch rate.*

A continuació enumerem els trets biomètrics més utilitzats, i comentem aspectes sobre la qualitat que tenen i l'ús que se'n fa:

- **Empremtes dactilars**. L'ús de les empremtes dactilars com a mitjà d'identificació és d'alta fiabilitat. Té bona acceptació i popularitat.

- **Ull**. La identificació d'un individu amb l'anàlisi de l'iris té una fiabilitat molt alta. El problema és la facilitat d'ús. L'anàlisi de la retina per a identificar l'individu és més complexa encara.

- **Forma de la mà**. Aquest sistema està bastant estès, però potser presenta una mica menys de fiabilitat que els anteriors. Aquest sistema és susceptible de tenir atacs, ja que no resulta difícil recrear la forma d'una mà usant un motlle.

- **Cara**. L'anàlisi de la cara, sia en 2D o en 3D, és un bon mitjà per a identificar un individu. Així i tot, sempre val més fer un estudi en 3D, ja que es milloren els resultats respecte al mer estudi d'una imatge en 2D, i es dificulta l'èxit d'atacs. El desavantatge dels equips de 2D és que el sistema no distingeix si el que captura és realment una cara o una fotografia d'una cara.

- **Venes del dit o la mà**. L'estudi vascular dels dits o de la mà proporciona alta fiabilitat i, a més, l'anàlisi no és gaire complexa.

- **Veu**. Aquest sistema presenta força fiabilitat, però també és susceptible als atacs. A més, té poca estabilitat, de manera que s'han d'analitzar unes quantes preses de veu per a reduir la taxa d'errors.

Clarament, hi ha més d'una característica biomètrica que es pot usar per a identificar o autenticar. Es poden usar individualment, o bé en combinació les unes amb les altres, o bé fent l'autenticació amb informació addicional, com és ara una contrasenya. La figura mostra un lector d'empremta digital per a ajudar a la identificació en un ordinador portàtil.

Lector d'empremtes dactilars d'un ordinador portàtil

2. Cicle de vida de la identitat digital

Una identitat digital passa per tres passos bàsics en el cicle de vida que té: la creació, l'ús i la desaparició o baixa. En aquest apartat estudiarem aspectes relacionats amb l'alta, l'ús i la baixa de les identitats digitals, i, en concret, les contrasenyes i els certificats.

2.1. Alta d'usuaris

L'alta d'un usuari és el procediment previ al fet que aquest usuari pugui utilitzar un servei o bé accedir a un sistema. Hi ha dues maneres amb les quals es pot donar d'alta en un sistema un usuari:

- **De manera presencial**. L'individu acudeix al gestor d'identitats del sistema o del servei (per exemple, a l'administrador dels equips informàtics d'una empresa), i aquest gestor li proporciona la informació necessària per a usar el servei. En aquest cas el gestor d'identitats ha identificat i autenticat l'usuari de manera presencial. La presencialitat és important en els sistemes o serveis amb riscos potencials.

Importància de la presencialitat

Obtenir un certificat digital o una targeta de coordenades per a operar amb una entitat financera poden ser un parell de situacions en què es requereixi presencialitat.

- **De manera no presencial**. En aquest cas l'individu tria (o li és assignat) un nom d'usuari, i també una contrasenya o una altra informació perquè es pugui autenticar. En aquest cas, útil i habitual en les situacions en què no hi ha grans riscos, s'ha de fer una sèrie de comprovacions per a millorar la seguretat del procés d'alta d'usuari.

2.1.1. Confirmació no presencial de la identitat

En la manera presencial, qui dóna d'alta l'identificador i la resta d'informació d'autenticació necessita la verificació visual que el sol·licitant és qui diu que és. No obstant això, tal com hem apuntat, en els sistemes no presencials s'han de prendre una sèrie de mesures per a evitar situacions com la suplantació d'identitat o l'accés indegut als sistemes.

Imaginem-nos que un usuari es vol donar d'alta en un servei telemàtic pel qual farà falta introduir una contrasenya com a sistema d'autenticació. L'usuari introdueix el seu identificador (del qual es comprova que no n'hi cap més d'igual en el sistema) i una contrasenya. Per a millorar l'alta d'usuari es poden usar aquestes eines:

- **Correu electrònic**. Es pot demanar a l'usuari que introdueixi una adreça de correu electrònic. En aquesta adreça, rebrà un correu que contindrà un enllaç a una pàgina que activa automàticament el compte d'usuari acabat

de crear. Ara bé, imaginem-nos el cas que el servei és una xarxa social. Com que no hi ha comprovació presencial, es podria usar una adreça de correu electrònic pròpia (de manera que l'activació tindria èxit), però, al mateix temps, crear un identificador per a emplenar el perfil de xarxa social d'un altre individu.

- **Telèfon mòbil**. Un altre sistema pot consistir a demanar un número de telèfon mòbil al qual el servei enviarà un codi d'activació. Clarament, com en el cas del correu electrònic, no s'evita la possibilitat de frau. No obstant això, amb la legislació actual es pot identificar el propietari del número del telèfon mòbil.

Autenticació per mòbil

El mitjà d'autenticació per telèfon mòbil és habitual per a la confirmació d'operacions de compra per Internet.

- **Confirmació per dades**. Si el sistema telemàtic es correspon amb una entitat que ha mantingut relació amb l'usuari prèviament, es poden demanar dades per a comprovar que la identitat del sol·licitant es correspon amb l'individu. Podria ser el cas de crear un accés a l'oficina virtual d'una companyia elèctrica: es podria demanar, per exemple, una quantitat determinada d'alguna de les factures emeses amb anterioritat.

Finalment, en molts casos es pretén evitar l'ús indegut del servei (per exemple, un servei de correu electrònic, un blog o un fòrum) o bé es vol protegir el sistema davant el bloqueig del servei. En el primer cas, un programa es podria donar d'alta automàticament en molts serveis per a inundar-los de publicitat. En el segon, el programa aniria fent peticions automàtiques i creant usuaris fins a col·lapsar el sistema. Per a evitar que un programa usi formularis pensats perquè els empleni un humà, s'usen les ***captcha***.

Captcha

Captcha és l'acrònim de *prova de Turing pública i automàtica per a diferenciar màquines i humans* o *completely automated public Turing test to tell computers and humans apart.*

Una *captcha* és una prova que en principi només pot ser resolta per humans, no per programes, i l'objectiu de la qual és diferenciar un humà d'un programa.

La típica prova és que l'usuari ha d'introduir per teclat una paraula o conjunt de caràcters que s'exposen per mitjà d'una imatge distorsionada, borrosa, amb soroll, etc., és a dir, amb qualsevol de les característiques que pugui dificultar a un programa la lectura automàtica però no a un humà.

Exemple de *captcha*

2.1.2. Contrasenyes, codis i recomanacions

Si creem un usuari, necessitem una contrasenya. Si rebem un certificat electrònic, és molt recomanable utilitzar una contrasenya o un codi per a protegir la clau privada corresponent al certificat. Així, doncs, en aquest subapartat tractarem d'alguns conceptes sobre les contrasenyes i altres codis d'autenticació.

D'entrada, vegem quines estratègies té un atacant per a intentar endevinar un codi o una contrasenya que li permetin suplantar una identitat:

- **Usar la força bruta**. Consisteix a provar totes les possibles combinacions de símbols vàlids fins a encertar el valor correcte.

- **Fer cerca intel·ligent**. Es tracta de buscar per un espai de noms restringit (per exemple, provar el número de telèfon de l'individu al qual es vol suplantar). Un d'aquests casos és l'atac de diccionari, consistent a buscar contrasenyes a partir d'un diccionari.

Afortunadament, es disposa d'una gran quantitat de consells i tècniques per a millorar la seguretat de la contrasenya:

- **Canviar la contrasenya per defecte**. Quan en el procés d'alta l'usuari no decideix quina és la seva contrasenya, el sistema li'n proporciona una. És molt recomanable que l'usuari la canviï per una que li sigui més fàcil de recordar, i que sigui "nova", tan aviat com li sigui possible.

- **Tenir en compte l'aspecte de la contrasenya**. És aconsellable una longitud mínima, i també la combinació de lletres (majúscules i minúscules), nombres i si pot ser altres caràcters. Malauradament, hi ha alguns sistemes que limiten el conjunt de caràcters possible, o fins i tot limiten la longitud màxima de la contrasenya. L'objectiu d'aquesta mesura és augmentar l'espai de cerca i dificultar les possibles repeticions de contrasenyes.

- **No usar contrasenyes òbvies**. És evident, sobretot per a evitar els atacs de cerca intel·ligent.

Contrasenyes òbvies a Hotmail

Després d'un atac massiu, es van revelar quines són les contrasenyes més usades a Hotmail. La clau que va aparèixer amb més freqüència va ser 123456. La notícia es pot llegir al web de RTVE.

- **Usar mesuradors de seguretat de contrasenya**. Hi ha molts sistemes que informen de la qualitat de la contrasenya triada, en relació amb la seguretat que ofereix. Aquests sistemes es basen en les recomanacions anteriors per a decidir sobre la seguretat de la contrasenya escollida.

- **Forçar periòdicament el canvi de contrasenya**. Si la contrasenya de l'usuari ha estat obtinguda per algun atacant, el canvi periòdic fa que la contrasenya usurpada ja no tingui validesa.

- **Permetre un nombre màxim d'intents fallits**. Amb aquesta tècnica es limita clarament l'èxit dels atacs de força bruta. Quan s'arriba al màxim d'intents es bloqueja el compte.

- **Sol·licitar codis d'autorització en les operacions que necessiten més seguretat**. Aquests codis se solen trobar en una targeta de coordenades específica de l'usuari, encara que també es pot usar un testimoni. En aquest cas és recomanable que el codi d'autorització sigui d'un sol ús.

Els consells anteriors són habituals en la majoria de sistemes de validació per mitjà de contrasenya. L'administrador del sistema ha de dissenyar un procés de gestió de contrasenyes que tingui en compte aquests aspectes. No obstant això, fins i tot prenent precaucions tècniques, el robatori de contrasenyes té un altre problema de seguretat: el robatori mitjançant un correu electrònic o una trucada telefònica fent-se passar per un administrador del sistema i demanant la contrasenya a un usuari incaut. Per a ser immune als atacs de pesca o *phishing*, s'ha de conscienciar l'usuari, perquè no n'hi ha prou de prendre mesures tecnològiques. A més de tot això, és essencial no apuntar contrasenyes en llocs visibles. Aquests punts són necessaris en qualsevol política de seguretat informàtica de qualsevol organisme o empresa.

2.2. Procediment d'autenticació

Quan un usuari s'ha donat d'alta en el servei, ja està a punt d'usar-lo. És llavors quan, concretament, es pot autenticar en el servei. Per exemple, pot usar el seu perfil de xarxa social, o bé pot accedir a fer un tràmit amb l'Administració.

El sistema ha de tenir en compte que l'usuari s'ha autenticat i està en una **sessió activa**. Els diferents sistemes operatius tenen implementat el control dels usuaris que estan actius, però això no ocorre en les aplicacions basades en el Web.

No és possible traslladar directament a les pàgines web el concepte de *sessió*, ja que el protocol HTTP[8] tracta les peticions que fa l'usuari de manera independent. Per a implementar el concepte de *sessió* en la tecnologia de pàgines web s'ha d'usar una galeta (*cookie*) de sessió.

[8] *HTTP* és la sigla de *protocol de transferència d'hipertext* o *hypertext transfer protocol*.

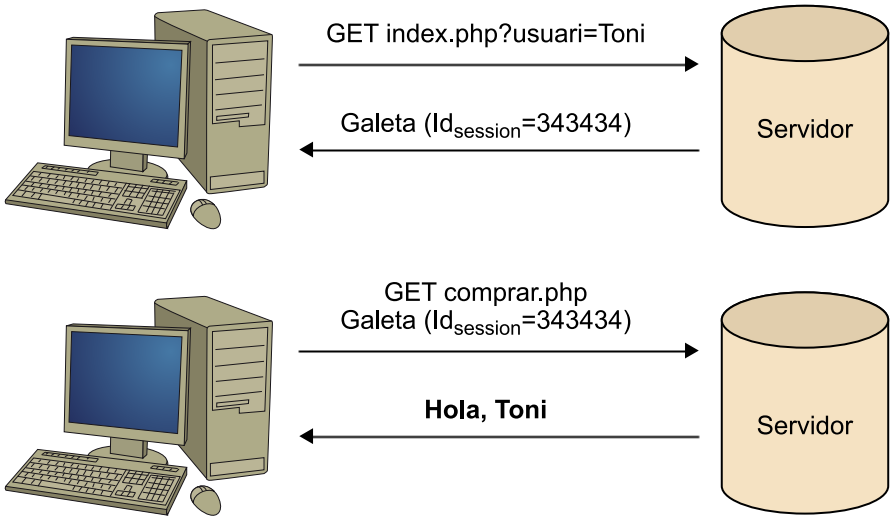
Sessions sense galetes

Es poden implementar sessions sense usar galetes: en aquest cas l'identificador de sessió és un paràmetre més de l'adreça web.

Una galeta és un fitxer de text que el servidor web guarda a la màquina client. Són els únics fitxers que, per defecte, es poden dipositar a l'equip client sense que l'usuari en sigui conscient.

Les galetes s'usen per a guardar informació variada sobre el client; per exemple, es poden guardar certes preferències d'aspecte d'un lloc web que té l'usuari. Mitjançant les **galetes de sessió**, es poden manejar sessions d'usuaris autenticats en pàgines web: quan l'usuari s'identifica correctament, li és assignat un número de sessió (una cadena de bits llarga i aleatòria). Aquest número de sessió se sol guardar en una galeta a l'ordinador client. Així, doncs, el servidor és capaç d'associar el client amb una determinada sessió.

Recordatori d'usuari mitjançant un identificador de sessió guardat a l'ordinador client



Dins d'una sessió hi ha dades el valor de les quals ha d'estar disponible durant tota la sessió: són les anomenades *variables de sessió*. Un llenguatge com PHP disposa d'eines per a començar una sessió (`session_start()`) i acabar una sessió (`session_destroy()`), i també eines per a controlar les variables de sessió.

2.2.1. Autenticació mitjançant contrasenya

En introduir el concepte de les contrasenyes hem suposat que el servidor guarda una llista de contrasenyes en clar, és a dir, sense codificar. És clar que aquestes contrasenyes s'han de guardar en un fitxer inaccessible per als usuaris no administradors. I al seu torn, l'administrador, en la responsabilitat del qual recau part de la seguretat en aquest cas, ha de ser molt caut perquè no hi hagi problemes de robatori de contrasenyes.

Les contrasenyes han d'estar guardades en un lloc segur dins del sistema d'informació (base de dades) de qui identifica. Així, doncs, una opció molt estesa és que, juntament amb la informació de l'usuari, no s'hi guarda la contrasenya, sinó un resum d'aquesta contrasenya. De manera que, quan un usuari introdueix una contrasenya, no es comprova que la contrasenya coincideixi amb l'emmagatzemada, sinó que es comprova que el resum de la contrasenya coincideixi amb el resum emmagatzemat de la contrasenya. Per a fer el resum se sol usar una funció criptogràfica unidireccional de resum. En alguns sistemes, el valor de contrasenya que es guarda no és un resum, sinó el resultat d'encriptar un vector de bits fix i conegut pel sistema, usant la contrasenya com a clau d'encriptació.

Funció criptogràfica de resum

Una funció criptogràfica de resum o *hash* retorna, a partir d'una entrada de longitud arbitrària, una seqüència de bits d'una longitud definida. Perquè sigui útil en seguretat computacional, a partir dels bits obtinguts no s'ha de deduir el valor d'entrada (és unidireccional). A més, un petit canvi en l'entrada s'ha de reflectir com un valor de sortida completament diferent. Aquestes funcions també posen en relleu que és molt complex

computacionalment trobar dues entrades que siguin diferents i donin lloc a una mateixa sortida. Alguns exemples de funcions de resum són SHA-1 o MD5.

Clarament, és probable que els sistemes que permeten recordar una contrasenya guardin la contrasenya sense resumir o sense encriptar.

Durant el procediment de validació per contrasenya, l'usuari envia una contrasenya al servei d'autenticació. En els primers sistemes, l'autenticació mitjançant serveis com Telnet propiciava l'enviament de la contrasenya sense encriptar. És a dir que qualsevol atacant, usant una eina d'escolta de xarxa (detector o *sniffer*), podia usurpar la contrasenya de l'usuari. Per a evitar-ho, s'usa la protecció de xarxa o de sessió, mitjançant tècniques criptogràfiques. Ara bé, tal com hem apuntat més amunt, actualment el robatori de contrasenyes sol tenir lloc mitjançant atacs de pesca.

Hi ha un últim tipus de problema, però, que s'ha de tenir en compte a l'hora d'autenticar-se amb contrasenya: un atacant pot tenir instal·lat un programa a l'equip del client que registri totes les pulsacions de teclat per a enviar-les després a l'atacant i analitzar-les.

Un enregistrador de teclat o *keylogger* és un sistema, generalment programari, l'objectiu del qual és registrar tot el que tecleja l'usuari del sistema on està instal·lat, amb finalitats d'usurpació de contrasenyes.

En general es tracta de programari, encara que també n'hi ha en forma de dispositiu maquinari, els quals es poden identificar fàcilment amb una inspecció visual. Per a defensar-se dels enregistradors de teclat, és habitual demanar a l'usuari que utilitzi el ratolí en lloc del teclat per a introduir una contrasenya, tal com es veu en la figura. En aquest cas, els caràcters per a escriure la contrasenya canvien de posició en cada accés d'autenticació, de manera que és més complex pensar en un enregistrador de ratolí o *mouselogger*. En aquest cas l'atacant ha de capturar la pantalla de l'usuari per a obtenir la informació (enregistrador de pantalla o *screenlogger*).

Entrada del PIN amb el ratolí per a evitar possibles enregistradors de teclat

2.2.2. Autenticació amb certificats electrònics

Els protocols i les especificacions SSL/TLS/WTLS[9] protegeixen la capa del transport de la informació entre clients i servidors web. L'ús, a més, està estès a l'enviament i la recepció de correu electrònic i, en general, a totes les aplicacions que necessiten seguretat. Proporcionen, bàsicament, el següent:

(9)*SSL* és la sigla de *capa de sòcol segur* o *secure socket layer*; *TLS*, de *seguretat de nivell de transport* o *transport layer security*; i *WTLS*, de *seguretat de nivell de transport sense fil* o *wireless transport layer security*.

- Confidencialitat entre client i servidor (per exemple, per a enviar informació com números de targeta de crèdit o contrasenyes).
- Autenticitat del servidor, usant un certificat electrònic de servidor com a mètode d'autenticació.
- Integritat de la informació.

A més, aquests sistemes permeten la identificació d'un client mitjançant el seu certificat. Com que es tracta d'especificacions i protocols molt semblants, es tendeix a parlar-ne com a *protocols SSL/TLS*.

Quan ens connectem a un lloc web segur (identificat mitjançant HTTPS[10]) té lloc una comunicació entre client i servidor destinada a crear un canal de comunicació segur.

(10)*HTTPS* és la sigla de *protocol segur de transferència d'hipertext* o *hypertext transfer protocol secure*.

En aquest exemple es resumeixen els missatges que es transmeten quan un client es connecta a un servei HTTPS autenticat amb un certificat de servidor:

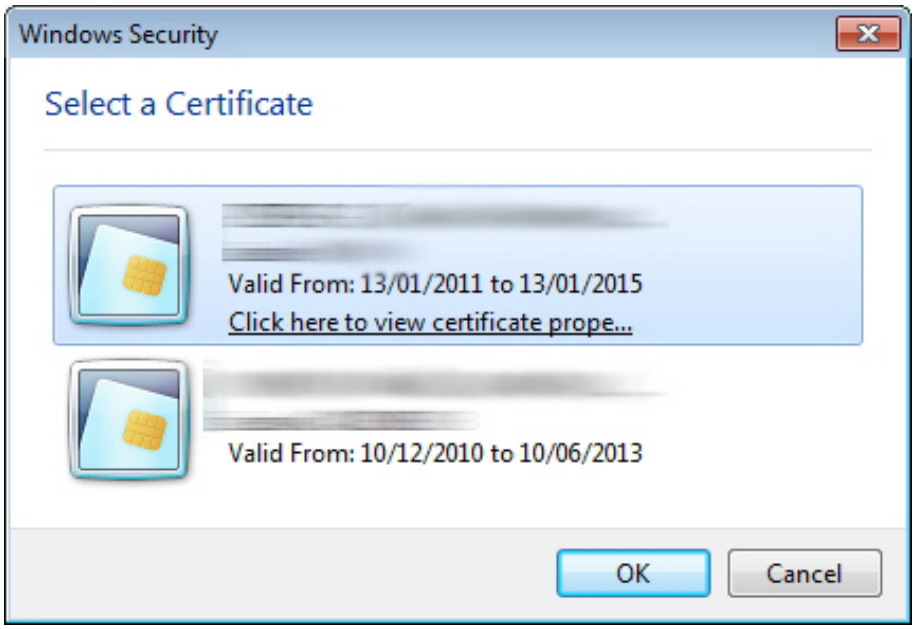
- *Hello request*. El servidor envia aquest missatge al client (el navegador web) per iniciar la protecció.
- *Client hello*. El client respon, donant una sèrie d'informació, com per exemple amb quins algorismes criptogràfics funciona (el servidor s'ha d'acomodar a una varietat de programari client amb diferents versions i sistemes operatius).
- *Server hello*. El servidor respon, i especifica quina combinació d'algorismes criptogràfics s'usarà.
- *Certificate*. El servidor envia el certificat de servidor que inclou una referència a l'emissor, amb la qual el client podrà decidir si confia directament en el certificat o no.
- *Server hello done*. A partir d'aquest missatge s'intercanvien les claus criptogràfiques i comença la comunicació segura.

Un cas una mica diferent és quan el servidor requereix que el client es validi usant un **certificat de client** (és el cas, per exemple, de la validació amb el DNIe). En el cas d'SSL, el servidor envia, abans del *Server hello done*, el missatge *Certificate request*. Aquest missatge conté una llista dels possibles tipus de certificat que admet el servidor, per ordre de preferència. També envia una llista d'autoritats de certificació. Així, doncs, el navegador carrega el certificat corresponent (en cas d'haver-hi diversos certificats de client, el sistema demana triar-ne un), tal com es veu en la figura.

Directiva *SSLVerifyClient require*

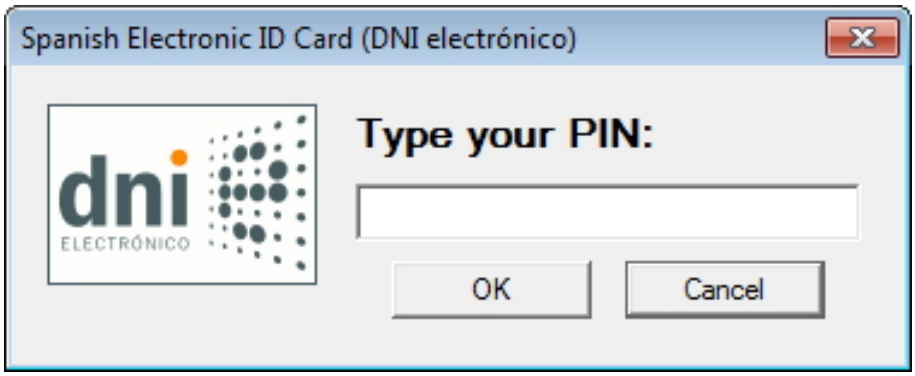
Es pot obligar el servidor Apache a l'autenticació del client mitjançant certificat amb la directiva *SSLVerifyClient require*.

Selecció de certificat electrònic a Windows 7



Per a usar el certificat, l'usuari ha de demostrar que és el propietari introduint el codi o la contrasenya corresponent.

Quadre de diàleg per a introduir la clau que permet usar el DNIe



Si la validació ha tingut èxit, s'envia el certificat mitjançant el missatge *Certificate*.

2.2.3. Autenticació *single sign-on*

Al principi de l'arribada d'Internet, els usuaris tenien pocs serveis davant els quals es poguessin autenticar. Avui dia, hi ha milers de llocs web que requereixen una autenticació de l'usuari perquè els pugui usar: el compte de correu, la xarxa social, el servidor de vídeos, l'espai de comentaris de la premsa, etc. D'altra banda, hi ha moltes empreses i organitzacions que tenen molts serveis propis o interns basats en el Web.

És clar que en tots dos escenaris els usuaris han de recordar molts noms i les respectives contrasenyes d'aquests noms per a utilitzar tots els serveis a què estan subscrits. Evidentment, el fet d'usar sempre la mateixa contrasenya per a tots els serveis planteja un problema: si un atacant obté la contrasenya la pot usar de manera deshonesta en tots els serveis.

Per a solucionar el fet que, dins d'una organització o un grup d'aplicacions basats en el Web, s'hagin d'usar molts noms d'usuari i contrasenyes, hi ha el procediment *single sign-on*.

Els sistemes *single sign-on* permeten l'accés a diversos serveis a partir d'un únic acte d'autenticació inicial.

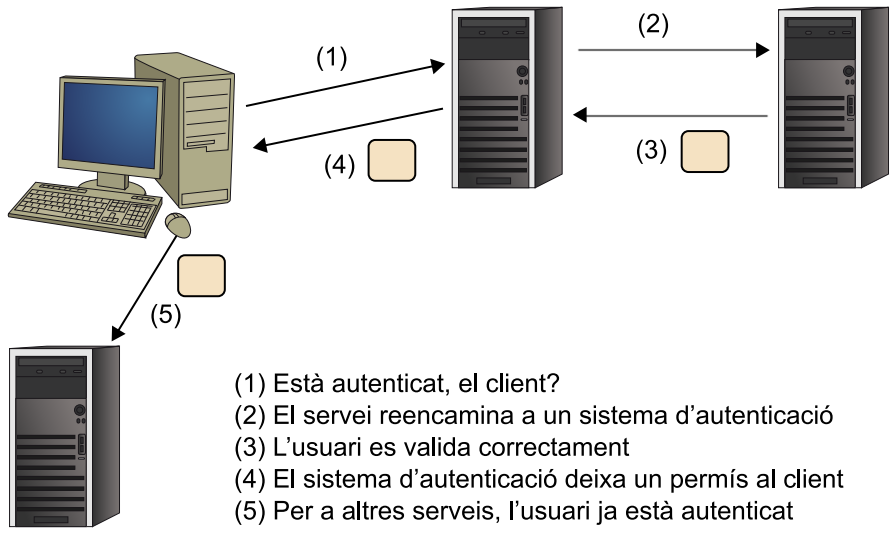
Exemple de sistema *single sign-on*

Una companyia ofereix un correu electrònic, un disc virtual, un calendari i un sistema d'elaboració cooperativa de documents per mitjà del Web. Quan l'usuari vol usar, per exemple, el calendari, s'ha d'autenticar davant el sistema. Amb això, com que no està autenticat, és reencaminat a un sistema autenticador. Si l'usuari es valida correctament, ja pot usar el calendari. Si l'usuari ara vol treballar amb un document en línia, no s'ha de tornar a autenticar. Probablement, el sistema d'autenticació li ha deixat en l'equip una galeta com a prova que l'usuari s'ha validat. Aquesta galeta té un període de validesa a partir del qual caduca la sessió i l'usuari s'ha de tornar a autenticar. La figura mostra aquest procediment:

Problema dels sistemes *single sign-on*

Òbviament, els sistemes *single sign-on* també permeten a un atacant accedir a molts serveis sabent una única contrasenya de l'usuari.

Procediment resumit d'autenticació *single sign-on*



2.3. Baixa d'usuaris

El cicle de vida d'una identitat digital s'acaba amb un procediment de baixa. Tot procés de gestió d'identitats ha de preveure com es fa aquest tràmit. A continuació comentem alguns aspectes referents a la baixa de contrasenyes i certificats electrònics.

2.3.1. Baixa de contrasenyes

Quan un individu ja no pot (o no vol) usar un servei telemàtic, s'ha de (o es pot) donar de baixa. En els sistemes gestionats per administradors, aquest procediment s'ha de fer quan es notifiqui el cessament de l'individu. Clarament, un individu que, per exemple, ja no treballa en una empresa, no ha de poder accedir als seus serveis telemàtics, com per exemple el correu electrònic o la intranet. Normalment, es pot definir un període breu durant el qual l'usuari encara està actiu en tots els serveis o alguns serveis. Per exemple, no pot accedir a la intranet, però sí continuar rebent correus electrònics al compte institucional (i potser ja no pot enviar correus des d'aquest compte).

En serveis gestionats automàticament, en general serveis amb una quantitat ingent d'usuaris, el procediment de baixa pot arribar a ser automàtic: quan un usuari es registra, li és advertit, per exemple, que caducarà el seu compte d'usuari si no ha fet cap activitat durant un determinat període. No és sobrer que, en un sistema d'aquest tipus, s'enviïn alguns missatges de recordatori a l'usuari abans que caduqui el compte.

2.3.2. Baixa de certificats electrònics

Pel que fa a certificats electrònics, la baixa de la identitat digital implica altres conceptes i escenaris:

- **Un certificat pot caducar**. Si la data en què s'usa un certificat està fora del període de validesa, s'avisa el propietari del certificat d'alguna manera. L'administrador d'un servei ha de preveure la caducitat dels certificats de servidor dels seus sistemes i renovar-los abans que caduquin per a no perjudicar els usuaris.

- **Un certificat veu compromesa la seguretat**. Per exemple, si es perd un DNIe o bé a l'usuari li sembla que hi ha hagut una usurpació de la clau privada o del codi d'accés, s'ha de fer una **revocació** del certificat.

> Un **certificat revocat** és un certificat considerat no vàlid encara que sigui emprat dins del període de validesa i l'emissor sigui de confiança.

Hi ha diferents tècniques per a tractar amb certificats revocats. D'entrada, l'usuari ha de demanar la revocació del certificat, mitjançant un tràmit amb l'emissor del certificat.

Ara bé, també és important que la revocació sigui notificada als potencials usuaris del certificat. Per a resoldre aquest problema tenim el concepte de **llista de certificats revocats** (CRL[11]). Una CRL conté **números de sèrie** de certificats revocats per la seva autoritat de certificació. Si es vol comprovar la validesa

(11) *CRL* és la sigla de *llista de certificats revocats* o *certificate revocation list*.

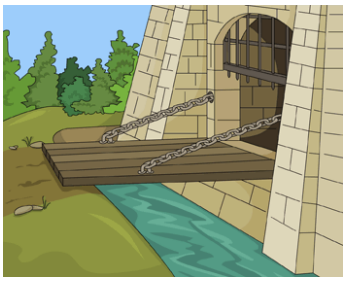
d'un certificat, s'ha de baixar una CRL actualitzada. L'adreça web per a baixar aquesta llista s'indica en un dels camps del certificat digital. La gestió de les CRL forma part de les plataformes PKI. Encara que les CRL són un mecanisme de comprovació àmpliament usat, l'obtenció i la interpretació de la llista de revocació implica certa complexitat. El protocol OCSP[12] és un protocol que informa de la validesa d'un certificat en concret: es fa una petició a un servidor OCSP *respondre* que ens informa de la validesa d'un certificat. Així, doncs, s'evita la baixada i la interpretació (*parsing*) d'una llista de certificats revocats.

(12)*OCSP* és la sigla de *protocol en línia de l'estat del certificat* o *online certificate status protocol.*

3. Control d'accés

Des de temps antics els humans s'han protegit a si mateixos i els seus recursos (aliments, eines, etc.) amb una gran varietat de sistemes. Probablement, una de les maneres més primitives de protegir les seves vides i els seus recursos van ser les coves, que els permetien protegir-se del fred i aixoplugar-se de la pluja i dels elements, i alhora dificultaven els atacs de depredadors. La grandària de les coves i, especialment, de les entrades que tenien resultava de vital importància per als primers humans. Hi ha diversos estudis que mostren que les coves amb entrades petites (més fàcils de controlar) eren usades per a fer activitats secretes (Holderness i altres).

El control d'accés ha estat històricament un problema eminentment físic. Muralles, fossats, ponts destructibles, ponts llevadissos, portes i reixats són solament alguns exemples d'elements arquitectònics que al llarg de la història han estat usats per a controlar l'accés a espais i recursos. El control d'accés entès des d'un punt de vista físic s'ha implementat en gran mesura amb l'ús de claus i portes. Els recursos s'emmagatzemen en àrees solament accessibles per mitjà de portes que únicament s'obren amb determinades claus. Així, solament els qui tenen les claus adequades poden accedir als recursos.



Durant l'edat mitjana era freqüent la protecció de castells i ciutats amb ponts destructibles o llevadissos que permetien travessar un fossat i entrar a un recinte sovint emmurallat.

Tot i que el control d'accés físic és encara una realitat ineludible. Qui no s'ha deixat mai les claus? Després de l'adveniment i la generalització posterior de les TIC, el control d'accés físic ha perdut protagonisme en favor del control d'accés lògic[13] o virtual, relacionat amb els sistemes de seguretat informàtica. En el text que hi ha a continuació ens centrarem en l'estudi del control d'accés entès des d'aquest punt de vista.

(13) *Lògic*, en el sentit informàtic del terme, en contraposició a *físic*.

El **control d'accés** és el procés pel qual, donada una petició de recursos, es permet o es nega l'accés a aquests recursos sobre la base de l'aplicació d'unes polítiques d'accés.

Vegeu també

El concepte de *polítiques d'accés* com a conjunt de regles que regeixen el control d'accés s'explica detalladament en el subapartat 3.2.

El control d'accés comprèn mecanismes d'autenticació, autorització i auditoria. Els objectius principals que té són protegir dades i recursos enfront de l'accés no autoritzat (protegir el secret) i enfront d'una modificació no autoritzada (protegir la integritat), i alhora garantir l'accés dels usuaris legítims als recursos (no-denegació del servei). Amb la finalitat d'aconseguir aquests objectius, es controlen tots els accessos al sistema i els recursos d'aquest sistema, i solament es permet que tinguin lloc els que són autoritzats. Fent un símil amb els sistemes físics, en concret els ponts llevadissos i els ponts destructibles, observem que aquests dos ponts compleixen els dos primers objectius (protegir

el secret i la integritat). En canvi, els ponts destructibles no satisfan el tercer objectiu ja que, quan són destruïts, no hi pot passar ningú, i provoquen així una denegació de servei per a les peticions autoritzades.

Els sistemes de control d'accés han de ser entesos com a mecanismes de monitoratge capaços d'interceptar totes les peticions de recursos que arriben al sistema. Aquests sistemes de control han de complir els requisits següents:

- **Resistència a manipulacions**. El sistema no pot ser alterat o manipulat i, si ho és, aquesta alteració ha de ser detectable. En el cas que no sigui així, el sistema no és segur, ja que pot permetre l'accés no autoritzat a recursos de manera inadvertida.

- **No eludible**. El sistema no pot ser saltat, és a dir, tot accés s'ha de produir per mitjà del sistema. En cas de no complir-se aquesta condició, el sistema no és segur, ja que hi haurà peticions de recursos que no seran analitzades i donaran lloc, així, a possibles accessos no autoritzats.

- **Seguretat nuclear**. La seguretat del sistema s'ha de concentrar en un nucli i no s'ha de distribuir pel sistema informàtic. Si no és així, tot el codi del sistema informàtic haurà de ser validat per tots els punts d'accés, i crearà així una sobrecàrrega innecessària.

- **Grandària petita**. El sistema ha de ser prou petit per a permetre la prova formal de la seva seguretat.

Demostracions formals

Gràcies a les demostracions formals podem provar les propietats de seguretat d'un model sense haver-lo d'implementar. Així, si el model és fidel a la realitat, el sistema resultant, després d'haver-lo implementat, manté les mateixes propietats de seguretat.

3.1. Fases del desenvolupament d'un sistema de control d'accés

El desenvolupament d'un sistema de control d'accés sol tenir les tres fases següents:

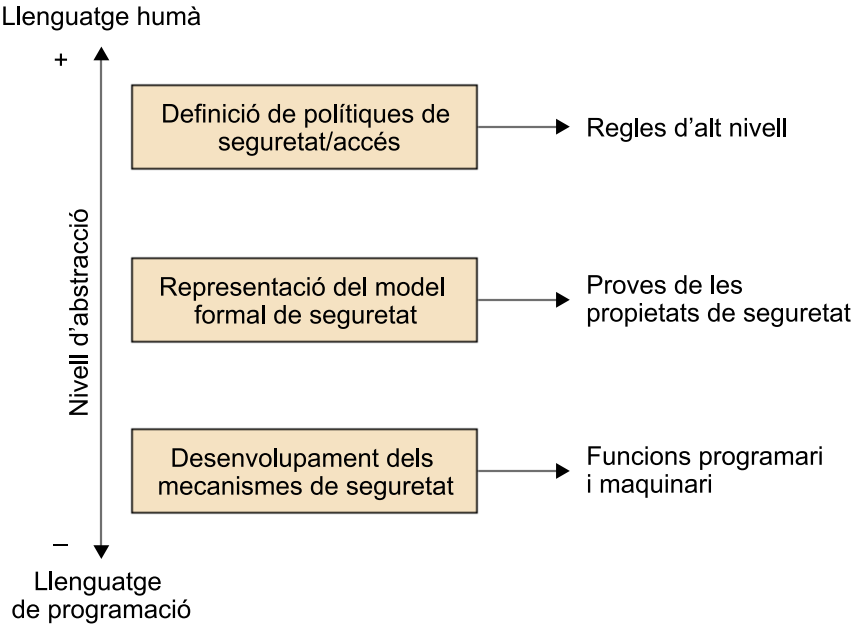
Polítiques de seguretat

Les polítiques de seguretat són el conjunt de regles que regulen l'accés als recursos del sistema.

1) La definició de les polítiques de seguretat
2) La representació mitjançant un model formal
3) La implementació dels mecanismes de seguretat

Les tres fases, que s'assemblen a les del procés de desenvolupament de programari, es mostren gràficament en la figura:

Abstracció i fases de desenvolupament d'un sistema de control d'accés



Durant la primera fase del procés (**definició de polítiques de seguretat**), s'estableix, amb llenguatge natural, el conjunt de regles que regulen l'accés als recursos del sistema de manera abstracta. En aquesta fase del procés, les regles poden ser vagues i fins i tot ambigües, ja que sovint fan referència a lleis, processos de funcionament propis i procediments d'organització. Aquesta ambigüitat fa que les regles, en aquesta fase, hagin de ser interpretades i no siguin aptes per a un sistema informàtic. Per exemple, podem considerar la regla "Tots els enginyers de nivell avançat tenen accés a l'ordinador central"; en aquest cas, "nivell avançat" és un concepte vague que posteriorment haurà de ser formalitzat.

En la segona fase del procés (**representació del model formal de seguretat**), es representa formalment el conjunt de regles i el funcionament que tenen. Aquesta formalització permet demostrar que un sistema compleix un determinat conjunt de propietats de seguretat. Un dels primers models de seguretat que es van proposar va ser el de Bell i LaPadula (Bell i LaPadula, 1973). El 1976 va aparèixer el model HRU de Harrison, Ruzzo i Ullmann que va formalitzar, entre altres qüestions, el concepte de *matriu d'accés* (Harrison i altres, 1976).

Vegeu també

El concepte de *matriu d'accés* s'explica detalladament en el subapartat 3.3.

Finalment, la tercera fase del procés (**desenvolupament dels mecanismes de seguretat**) consisteix en la implementació del model mitjançant l'ús de llenguatges de programació que són interpretats de manera determinista i sense ambigüitat per un sistema informàtic.

3.2. Polítiques d'accés: concepte i elements bàsics

Tot sistema de control d'accés considera els elements bàsics següents:

- **Objectes** (anomenats també *objectius*). Són totes les entitats d'un sistema susceptibles de ser protegides. En el cas d'un sistema operatiu, són arxius, directoris, programes, dispositius, terminals, ports, etc. En el cas d'una base de dades, hi tenim taules, relacions, vistes, procediments, etc.

- **Accions**. És tot allò que es pot fer sobre un objecte. Les accions típiques que podem fer sobre un fitxer són lectura, escriptura, creació i eliminació. En cas que l'objecte sobre el qual es fa l'acció sigui un programa, s'hi ha d'afegir l'opció d'execució.

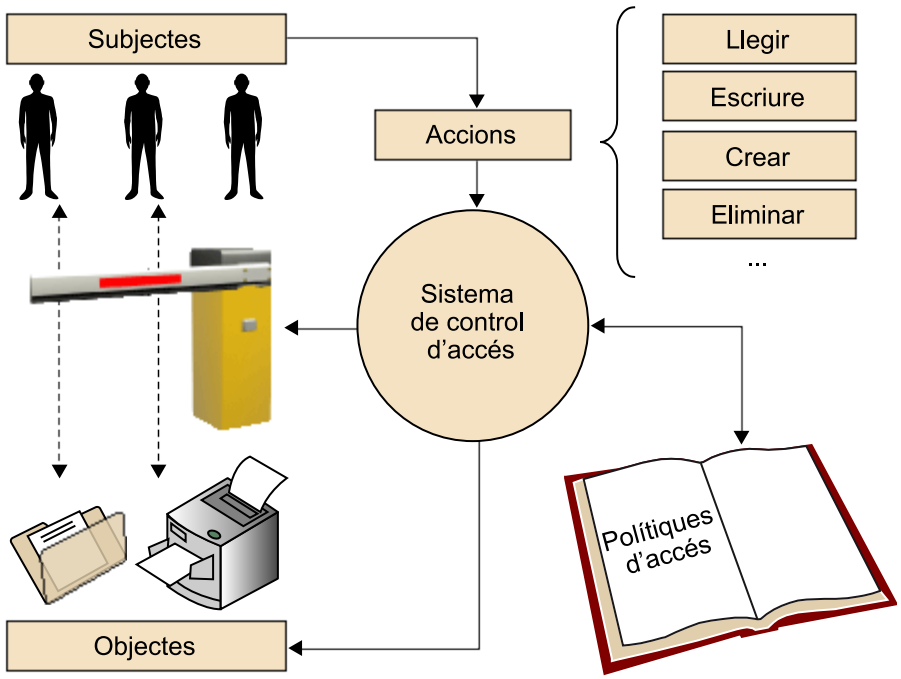
- **Subjectes** (anomenats també *iniciadors*). És qualsevol entitat amb capacitat de requerir l'accés a objectes del sistema. Els subjectes típics d'un sistema són els usuaris i els processos del sistema (per exemple, un navegador web o un processador de textos).

En tot sistema informàtic, els subjectes duen a terme accions sobre els objectes. El sistema de control d'accés és l'encarregat de decidir si un determinat subjecte té permís per a executar una determinada acció sobre un determinat objecte. La decisió de permetre o denegar l'accés als recursos es fa sobre la base de les polítiques d'accés.

Les **polítiques d'accés** són el conjunt de regles que permeten determinar si un subjecte pot fer una determinada acció (lectura, escriptura, modificació, eliminació o execució) sobre un objecte.

La figura mostra un esquema dels components principals d'un sistema i la interacció que tenen amb el sistema de control d'accés. Fixem-nos que el sistema de control d'accés (al mig de la figura) rep peticions dels subjectes per a dur a terme accions. Avalua aquestes peticions amb l'ús d'una política d'accés i actua en conseqüència permetent o denegant l'accés als objectes.

Elements bàsics d'un sistema de control d'accés i la interacció d'aquests elements



3.3. Tipus de control d'accés

Segons com s'apliquen i es gestionen les polítiques d'accés, distingim tres tipus fonamentals de control d'aquest accés:

1) Control d'accés obligatori. Les polítiques són avaluades pel sistema entès com un únic ens central. Els subjectes del sistema no poden refer o redefinir les polítiques. Per exemple, no poden donar permisos d'accés a altres usuaris. Els objectes i els subjectes del sistema pertanyen a diverses classes d'accés. Així, per a accedir a un objecte d'una determinada classe cal que el subjecte pertanyi a una classe igual o superior (en termes de privilegis). Aquest tipus d'accés s'inspira en el funcionament militar, en què la informació (per exemple, plans d'atac) solament la poden veure les persones que tenen un nivell de seguretat suficient (per exemple, nivell de coronel).

2) Control d'accés discrecional. Les polítiques són gestionades pels propietaris (subjectes) dels recursos (objectes). Els subjectes poden modificar les polítiques associades als objectes del sistema. Per exemple, un propietari d'un determinat objecte del sistema pot donar privilegis d'accés sobre aquest objecte a un altre subjecte. Aquest tipus de control d'accés és usat generalment pels sistemes operatius.

3) Control d'accés basat en rols. Les polítiques són definides pel sistema, però, a diferència de les polítiques d'accés obligatori, l'accés no s'avalua segons permisos individuals sinó mitjançant permisos de classe (o de rol). Cada rol té assignats certs privilegis i cada subjecte del sistema té assignat un rol; així, el

Nota

El control d'accés obligatori i el control d'accés discrecional es poden veure com a casos particulars d'un model de control d'accés basat en rols.

subjecte adquireix els privilegis del rol a què pertany. Aquest tipus de control d'accés és un cas general dels dos anteriors. Se sol usar per a la gestió d'accés a recursos de bases de dades.

En els subapartats següents descriurem amb més detall les característiques d'aquests sistemes de control d'accés i d'alguns altres de menys habituals.

3.3.1. Control d'accés obligatori

En un sistema de control d'accés obligatori (MAC[14]), les polítiques són avaluades de manera centralitzada per una autoritat (en el cas d'un sistema operatiu, l'encarregat és al nucli del sistema). En general s'usen sistemes de seguretat multinivell basats en classificacions dels subjectes i els objectes del sistema. Tots els subjectes i els objectes tenen assignada una **classe d'accés**.

(14)*MAC* és la sigla de *control d'accés obligatori* o *mandatory access control*.

Una **classe d'accés** és un element d'un conjunt de classes ordenat parcialment, en el qual l'ordre la dóna una relació de dominància representada per ≥.

En la forma més simple que té, un conjunt de classes d'accés es defineix amb un conjunt d'etiquetes ordenades. No obstant això, en general, les classes d'accés estan caracteritzades per dos components:

- **Nivell de seguretat (*N*)**. És un element d'un conjunt jeràrquic ordenat. Per exemple, podem considerar els elements seguretat alta (*SA*), seguretat mitjana (*SM*) i seguretat baixa (*SB*), en què $SA > SM > SB$.

- **Conjunt de categories (*C*)**. És un subconjunt d'un conjunt no ordenat els elements del qual fan referència a àrees funcionals o de competència. Per exemple, podem considerar els elements gestió, investigació, transferència i docència. En aquest cas l'element gestió es pot associar a objectes relacionats amb l'administració, la comptabilitat i els recursos humans, mentre que els elements investigació o transferència es poden associar amb objectes relacionats amb laboratoris o equips informàtics.

A partir d'aquests dos components (nivell de seguretat i conjunt de categories), podem definir la relació de dominància de la manera següent:

Classes incomparables

Donades dues classes, c_1 i c_2, si no es compleix que $c_1 \geq c_2$ ni que $c_2 \geq c_1$, es diu que les classes són incomparables.

La classe $c_1 \geq$ que la classe c_2 si el nivell de seguretat de c_1 és més gran que el nivell de seguretat de c_2 i el conjunt de categories de c_1 inclou el conjunt de categories de c_2. Formalment:

$$\forall\ c_1 = (N_1, C_1),\ c_2 = (N_2, C_2):\ c_1 \geq c_2 \Leftrightarrow N_1 \geq N_2 \wedge C_1 \supseteq C_2$$

La relació de dominància definida més amunt compleix les propietats reflexiva, transitiva, antisimètrica, existència de cota superior i existència de cota inferior.

Lectura recomanada

Si esteu interessats a aprofundir en les propietats de la relació de dominància, consulteu l'obra de Samarati i altres (2001).

La classe d'accés associada a un objecte indica la **sensibilitat** de la informació continguda en l'objecte.

La **sensibilitat** d'una determina informació es pot entendre com el dany potencial que pot causar la revelació no autoritzada d'aquesta informació.

D'altra banda, la classe d'accés associada a un subjecte indica el nivell que té d'autorització formal o *clearance*.

L'**autorització formal** fa referència al nivell de confiança en un subjecte. Es pot veure com la confiança que es té que el subjecte no revelarà informació sensible a subjectes sense autorització.

Així, doncs, el control d'accés obligatori equival a la restricció d'accés a objectes basada en la sensibilitat de la informació continguda en els objectes i l'autorització formal dels subjectes per a accedir a una informació d'aquest nivell de sensibilitat.

3.3.2. Control d'accés discrecional

El **control d'accés discrecional** (DAC[15]) va ser definit pel Trusted Computer System Evaluation Criteria el 1985. Es basa a avaluar quin subjecte fa la petició d'accés als recursos i en un conjunt de regles d'accés explícites definides pels propietaris (*owners*) dels objectes. En un sistema DAC, tot objecte té un propietari, que és qui gestiona l'accés a aquest sistema.

(15)*DAC* és la sigla de *control d'accés discrecional* o *discretionary access control*.

Rep el nom de *discrecional* pel fet que els usuaris del sistema tenen la capacitat de transferir els seus privilegis d'accés a altres usuaris. A diferència del control d'accés obligatori, el model DAC no usa un sistema centralitzat en què solament una autoritat atorga i revoca privilegis d'accés als recursos. En conseqüència, cal l'ús de polítiques d'administració.

En els sistemes DAC les **polítiques d'administració** regulen els processos de gestió de privilegis (per exemple, transmissió o revocació) entre els subjectes del sistema.

Model HRU

El model de matriu d'accés va ser formalitzat per Harrison, Ruzzo i Ullmann i es coneix com a *model HRU*.

Una de les maneres més comunes de definir els permisos que té cada subjecte sobre cada objecte és el model de matriu d'accés (proposat en el model HRU). Aquest model, que al començament va ser descrit per Lampson en el context dels sistemes operatius i més endavant va ser refinat per Graham i Denning, permet descriure el control d'accés discrecional. Rep el nom de *model de matriu d'accés* perquè usa una matriu per a codificar l'estat de l'accés als recursos en tot moment. Concretament, cada cel·la M (i, j) de la matriu conté les accions que pot fer el subjecte (i) sobre l'objecte (j).

Exemple de matriu d'accés

La taula mostra un exemple de matriu d'accés en la qual es pot identificar tres subjectes (Ana, Bernardo i Carlos), que poden ser usuaris del sistema, i quatre objectes (*Arxiu1*, *Arxiu2*, *Executable1* i *Executable2*). Si ens fixem en la cel·la de la matriu corresponent a la intersecció entre el subjecte (Ana) i l'objecte (*Arxiu2*), veiem que les accions permeses són lectura i escriptura. A més, hi observem que Ana és la propietària de l'*Arxiu2*, cosa que li confereix la potestat d'atorgar privilegis sobre aquest objecte a altres subjectes del sistema.

Exemple de matriu d'accés

	Arxiu1	***Arxiu2***	***Executable1***	***Executable2***
Ana	Lectura Escriptura	Lectura Escriptura Propietat		Execució
Bernardo		Lectura	Execució	
Carlos				Execució

L'estat de la matriu d'accés pot ser modificat amb l'ús d'ordres que executen funcions primitives sobre l'estat de les autoritzacions. Concretament, el model HRU considera sis funcions primitives:

- Addició i supressió de subjectes
- Addició i supressió d'objectes
- Addició i supressió de privilegis

La representació de la matriu d'accés en la forma més simple que té, és a dir, amb una taula bidimensional, resulta altament ineficient quan creix el nombre de subjectes i objectes del sistema.

Fixem-nos que si el nombre de subjectes i objectes és gran, és probable que la majoria de les cel·les de la matriu siguin buides (ja que no tots els subjectes tenen accés a tots els objectes). Per això s'usen formes de representació alternatives espacialment més eficients com les següents:

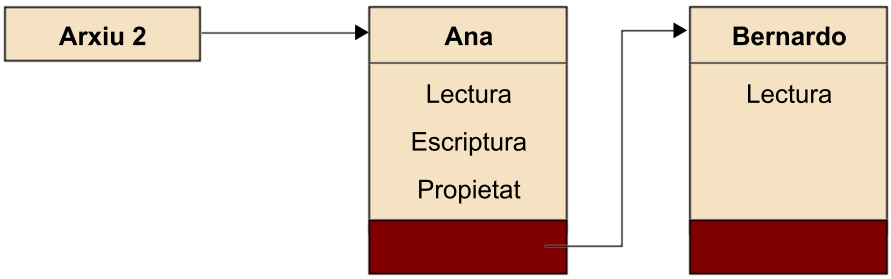
1) Taules d'autorització. Són taules amb tres columnes (subjecte, acció, objecte) que inclouen totes les cel·les no buides de la matriu d'accés. Així, cada registre de la taula representa la capacitat que té un subjecte de fer una acció sobre un objecte. La taula següent mostra la representació amb una taula d'autorització de la matriu d'accés de la taula anterior:

Representació amb una taula d'autorització

Subjecte	Acció	Objecte
Ana	Lectura	*Arxiu1*
Ana	Escriptura	*Arxiu1*
Ana	Lectura	*Arxiu2*
Ana	Escriptura	*Arxiu2*
Ana	Propietària	*Arxiu2*
Ana	Execució	*Executable2*
Bernardo	Lectura	*Arxiu2*
Bernardo	Execució	*Executable1*
Carlos	Execució	*Executable2*

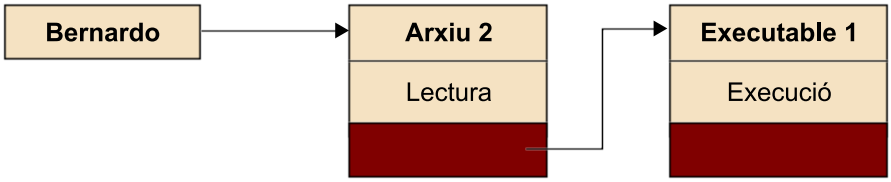
2) Llistes de control d'accés. Són llistes enllaçades que representen la matriu d'accés per columnes. D'aquesta manera, donat un determinat objecte (per exemple, l'*Arxiu2*) es pot determinar si un subjecte (per exemple, Bernardo) té permís per a fer alguna acció sobre aquest objecte (per exemple, llegir-lo). El gràfic mostra la llista de control d'accés per a l'*Arxiu2* segons la matriu d'accés d'exemple de la primera taula del nostre exemple.

Exemple de llistes de control d'accés



3) Llistes de capacitats. Són llistes enllaçades que representen la matriu d'accés per files. D'aquesta manera, donat un determinat subjecte (per exemple, Bernardo) es pot determinar si pot fer una acció (per exemple, execució) sobre un determinat objecte (per exemple, l'*Executable1*). El gràfic mostra la llista de capacitats de **Bernardo** segons la matriu d'accés d'exemple de la primera taula.

Llista de capacitats



3.3.3. Control d'accés basat en rols

Quan es treballa amb organitzacions grans resulta poc pràctic haver de definir els privilegis d'accés de manera individualitzada.

Exemple

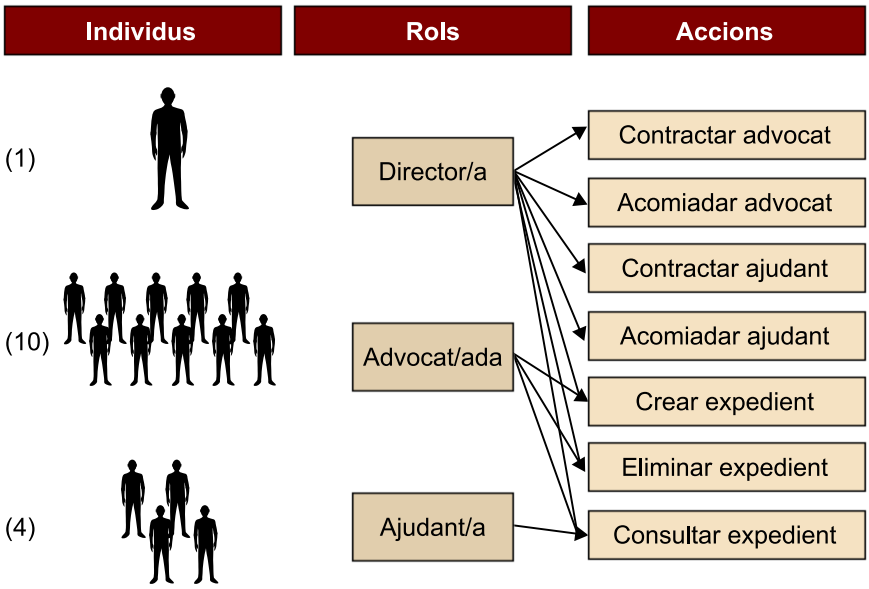
Prenguem com a exemple un bufet d'advocats format per quinze treballadors, un dels quals és el director, deu són advocats i quatre són ajudants. Imaginem-nos que les accions que es fan en el bufet són les següents:

- Contractar o acomiadar advocats.
- Contractar o acomiadar ajudants.
- Crear o eliminar expedients.
- Consultar expedients.

Al bufet, el director pot fer totes les accions, els advocats poden crear, eliminar i consultar expedients i els ajudants solament poden consultar els expedients.

La figura mostra gràficament els usuaris (treballadors) del bufet, els seus rols i les accions que poden fer. És fàcil observar que la definició de les accions que pot fer cada treballador de l'empresa és més còmoda si es considera el rol que exerceix a l'empresa (i per tant, les tasques que fa). Per exemple, no cal definir les accions que pot fer cada advocat de manera individual, sinó que simplement cal definir quines accions pot fer un advocat "genèric".

Usuaris, rols i accions per a l'exemple del bufet d'advocats



El **control d'accés basat en rols** (RBAC[16]) es fonamenta en la idea d'assignar permisos o privilegis per a fer accions a rols en comptes de fer-ho a subjectes del sistema. Així, cada subjecte del sistema té un rol assignat i pot fer totes les accions per les quals el seu rol té privilegis.

(16) *RBAC* és la sigla de *control d'accés basat en rols* o *role-based access control.*

Un **rol** és la funció que compleix algú o alguna cosa. Per exemple, en els sistemes operatius se sol fer una clara distinció entre el rol d'administrador i el rol d'usuari bàsic.

Fixem-nos que la gestió dels permisos se simplifica clarament respecte als models anteriors ja que, una vegada assignats els permisos als rols, l'única tasca consisteix a assignar correctament els rols als subjectes del sistema.

El model de control d'accés basat en rols és prou flexible per a funcionar com el control d'accés obligatori i el control d'accés discrecional. En realitat podem considerar que tant el model MAC com el DAC són casos particulars del model RBAC.

Resum

En aquest mòdul hem estudiat el concepte d'*autenticació de la identitat* i hem revisat quines són les tècniques bàsiques per a implementar-la, el cicle de vida de la identitat digital i el control d'accés.

D'entrada, hem vist l'ús de contrasenyes per a l'autenticació dels usuaris. Hem estudiat el concepte de *certificat electrònic*, revisant de manera resumida el concepte de *clau pública* i les propietats de seguretat de la informació que permet aconseguir. El concepte de *certificat electrònic* ha servit per a presentar el concepte de *signatura electrònica*, de la qual hem estudiat aspectes legals i d'implementació amb XML. També hem fet un repàs dels dispositius d'usuari per al suport als processos d'autenticació, veient diferents tipus de testimonis. Hem presentat el concepte de *targeta intel·ligent* i n'hem detallat l'ús en el DNIe. Finalment, hem presentat la biometria com un conjunt de tècniques capaces d'identificar individus o bé ajudar a autenticar-los.

També hem exposat el tema del cicle de vida de la identitat digital, estudiant conceptes com la gestió i la creació de contrasenyes, els problemes que comporta això i les possibles solucions que hi ha. Hem vist detalladament els processos d'autenticació amb certificats electrònics i hem introduït el concepte de *single sign-on*, que es veurà en més detall en el mòdul "*Single sign-on* i federació d'identitats". Finalment, hem tractat de la baixa d'usuaris, des del punt de vista d'usuaris autenticats amb contrasenya i des del punt de vista de revocar certificats electrònics.

A continuació hem estudiat els sistemes de control d'accés. Després de presentar el concepte des d'un punt de vista històric i mostrar-ne el vessant més físic, hem descrit com l'aparició de les TIC ens obliga a estudiar els sistemes de control d'accés des d'un punt de vista de seguretat informàtica.

Finalment, hem analitzat el concepte de *política d'accés* i hem descrit els principals actors que formen part del sistema, és a dir, objectes, subjectes i accions. Hem presentat els tres tipus fonamentals de control d'accés, a saber, control d'accés obligatori (MAC), control d'accés discrecional (DAC) i control d'accés basat en rols (RBAC).

Activitats

1. Busqueu per Internet alguns dels països que hagin integrat els certificats digitals en els seus sistemes d'identificació ciutadana. Elaboreu una llista de quins serveis ofereixen en general i reuniu dades sobre l'acceptació que han tingut.

2. Reuniu informació sobre la manera com se signen electrònicament alguns dels formats de document ofimàtic més comuns.

3. Busqueu alguna aplicació biomètrica de programari lliure o de demostració que pugueu provar. Instal·leu-la i feu diverses proves per a determinar-ne la taxa d'encerts i fallades.

4. Visiteu diversos webs financers, de comerç electrònic, etc., i enumereu els sistemes d'autenticació que admeten. En cas d'usar contrasenyes, tingueu en compte si s'usen algunes de les tècniques detallades en el mòdul.

5. Mireu d'obtenir un certificat de servidor d'algun web que sapigueu que usa SSL. Observant els detalls (o propietats, segons el programari que useu), intenteu obtenir l'URL de la llista de revocació. Introduïu aquest URL a la barra del navegador. Analitzeu la informació que conté la llista de revocació.

6. Escolliu un sistema operatiu actual (Linux, Windows o MacOS) i determineu quin tipus de control d'accés utilitza.

7. A partir de la següent matriu de referència d'accés, identifiqueu els objectes del sistema i els subjectes del sistema, i descriviu quines accions pot fer cada subjecte sobre cada objecte.

	Arxiu1	***Arxiu2***	***Executable1***	***Executable2***
Procés1	Lectura Escriptura Esborrament	Lectura Escriptura Esborrament Propietat		Execució
John	Lectura	Lectura		Execució
Julia	Lectura Escriptura Esborrament Propietat		Execució	Execució

8. Representeu la matriu d'accés anterior mitjançant la tècnica de taula d'autorització i de llista de capacitats.

9. Mostreu la matriu d'accés per a l'exemple del bufet d'advocats del subapartat 3.3.3. Argumenteu per què simplifica la gestió dels privilegis d'accés l'ús de rols.

10. A més dels tres models de control d'accés descrits en aquest mòdul (MAC, DAC i RBAC), hi ha altres models com l'ABAC (*attribute based access control*). Busqueu informació sobre aquest model de control d'accés i proporcioneu exemples de la manera d'usar-lo amb el llenguatge XACML.

Glossari

autoritat de certificació *f* Emissor de certificats electrònics que gaudeix de reconeixement sobre la seva confiança.

autorització formal *f* Nivell d'autorització o confiança en un subjecte. Es pot veure com la confiança que es té que el subjecte no revelarà informació sensible a subjectes sense autorització.
en clearance

biometria *f* Aplicació de les matemàtiques i la ciència de la computació per a identificar individus d'acord amb els seus trets o característiques físics.

captcha *f* Prova basada a reconèixer el text en una imatge i que té l'objectiu de diferenciar si qui la resol és un humà o un programa informàtic.

classe d'accés *f* Element d'un conjunt de classes ordenat parcialment, en el qual l'ordre la dóna una relació de dominància representada per ≥.

clearance *f* Vegeu **autorització formal**.

contrasenya *f* Cadena de caràcters alfanumèrics de longitud arbitrària, usada com a eina bàsica d'autenticació d'identitat.

control d'accés *m* Procés pel qual, donada una petició de recursos, es permet o es nega l'accés a aquests recursos sobre la base de l'aplicació d'unes polítiques d'accés.

infraestructura de clau pública *f* Plataforma informàtica o telemàtica que permet l'emissió i la gestió de claus criptogràfiques i els corresponents certificats d'aquestes claus.
en public key infrastructure

model HRU *m* Model de Harrison, Ruzzo i Ullman.

política d'accés *f* Conjunt de regles que permeten determinar si un recurs pot ser vist, llegit, modificat, eliminat o executat per un subjecte del sistema.

política d'administració *f* Conjunt de regles que regulen els processos de gestió de privilegis (transmissió, revocació, etc.) entre els subjectes d'un sistema de control d'accés discrecional.

public key infrastructure *f* Vegeu **infraestructura de clau pública**.

revocació *f* Procés mitjançant el qual un certificat electrònic perd la validesa, malgrat que no estigui caducat per data i que estigui emès per una autoritat de confiança.

rol *m* Funció que compleix algú o alguna cosa.

signatura electrònica reconeguda *f* Signatura electrònica creada per mitjans que el signant pot mantenir sota el seu control exclusiu, basada en un certificat reconegut. S'equipara completament a la signatura manuscrita.

sensibilitat *f* Dany potencial que pot causar la revelació no autoritzada d'una determinada informació.

sessió *f* Període durant el qual un usuari està autoritzat a dur a terme accions en una aplicació basada en el Web.

targeta intel·ligent *f* Targeta de plàstic que porta un xip incorporat, en general amb capacitats de microprocessador amb funcions criptogràfiques. El dispositiu és segur contra manipulacions.

testimoni *m* Dispositiu l'objectiu del qual és donar suport al procés d'autenticació de l'usuari. Es pot portar a sobre.
en token

token *m* Vegeu **testimoni**.

XAdES *m* Sistema estàndard de signatures electròniques mitjançant tecnologia XML. Reconegut com a estàndard en la Directiva europea per a la signatura electrònica.

Bibliografia

Bell, D. E.; LaPadula, L. J. (1973). "Secure Computer Systems: Mathematical Foundations". *MITRE Technical Report 2547* (vol. 1). [Versió digital actualitzada per Len LaPadula el 1996.]

Departament de Defensa dels EUA (1985). *Trusted Computer System Evaluation Criteria*. DoD Standard 5200.28-STD.

Gollmann, D. (2005). *Computer Security* (2a. ed.). Chichester (West Sussex): John Wiley & Sons.

Harrison, M. A.; Ruzzo, W. L.; Ullman, J. D. (1976). "Protection in Operating Systems". *Communications of the ACM* (núm. 19, vol. 8, pàg. 461-471).

Herrera Joancomartí, J. (2006). *Aspectos avanzados de seguridad en redes*. Barcelona: Editorial UOC.

Holderness, H. i altres (2006). *A Conservation Audit of Archaeological Cave Resources in the Peak District and Yorkshire Dales*. Document tècnic. CAPRA.

ISO (2009). *Common Criteria for Information Technology Security Evaluation* (ISO-IEC-15408).

Samarati, P.; Capitani di Vimercati, S. de (2001). "Access Control: Policies, Models, and Mechanisms". *FOSAD. Lecture Notes in Computer Science* (vol. 2171/2001, pàg. 137-196).

Stallings, W. (2008). *Computer security: principles and practice*. Upper Saddle River, NJ: Pearson / Prentice Hall.

Windley, P. (2005). *Digital Identity*. Sebastopol, CA: O'Reilly.