ДИГИТАЛНА ЗАШТИТА

Дигитална застита дели се на:

1. Дигитални потпис
2. Дигитални водени зиг
3. Интелигентне картице
4. Биометриски безбедносни механизми

ДИГИТАЛНИ ПОТПИС

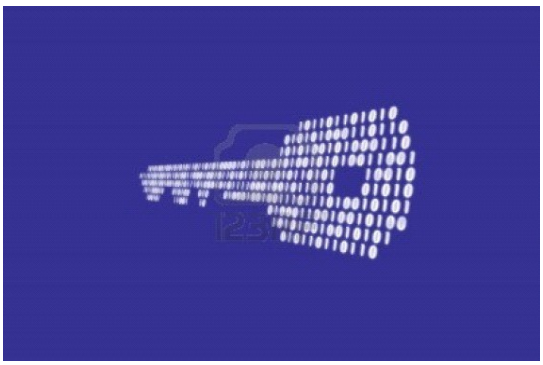
Порука се може и дигитално оверити тако што пошиљалац користи свој тајни кључ за оверу - како свог идентитета, тако и садржаја поруке, чиме се спречава било каква измена поруке током преноса. Ако би неко неовлашћено дописао или изменио садржај поруке, прималац би уз помоћ јавног кључа пошиљаоца открио нерегуларност у поруци, што значи да је дошло до неауторизоване измене поруке.

Дигитални потпис повећава интегритет података. Њиме се, на пример, потврђује пристанак на одређену пословну трансакцију. Дигитални потпис показује да је документ који сте послали ваш и да је непромењен стигао до крајњег одредишта.

Дигитални потпис реализује се на следећи начин:

Креирамо неки документ. На основу нашег приватног кључа, софтверски механизам заштите генерише запис као дигитални потпис који се додаје креираном документу. Треба истаћи да тај додатак важи само за конкретни документ. Ако би неко изменио само једно слово у том документу, дигитални потпис више не би одговарао, што значи да се дигитални потпис не може украсти и искористити за лажну оверу неког другог документа.

Крајњи корисник, који је добио документ уз помоћ нашег јавног кључа, добија потврду да смо га заиста ми написали.



ДИГИТАЛНИ ВОДЕНИ ЖИГ

Дигитална документа веома је лако копирати или модификовати, што погодује експанзији примене дигиталних докумената. Међутим, наведене предности истовремено представљају и велику опасност, пре свега због могућег злонамерног мењања садржаја мултимедијалних докумената, као и због недозвољеног копирања и угрожавања ауторских права.
Дигитални водени жигови су електронски еквивалент класичног воденог жига на документима као што су новчанице, чиме се остварује заштита од неовлашћеног копирања и истовремено доказује власништво или ауторство. Дигитални водени жигови представљају скривену поруку која се уграђује у сам мултимедијални документ.
Постоје две врсте дигиталних водених жигова - видљиви и невидљиви. Видљиви се, као што им и само име каже, могу лако уочити, али тешко уклонити из електронског документа. Насупрот њима, невидљиви су сакривени у садржају и представљају форму невидљивог "информационог жига". Обе врсте дигиталних водених жигова омогућавају њиховим ауторима да докажу своје власништво, и то не само над оригиналним документом, већ и на модификованим копијама које су саставни део неких других докумената.

ИНТЕЛИГЕНТНЕ КАРТИЦЕ

Аутентификација подразумева доказивање идентитета корисника. Идентитет у оквиру Интернета најчешће се доказује корисничким именом и лозинком, односно тајним кључем, а у последње време и интелигентним картицама (smart cards), као савременијим и ефикаснијим механизмом заштите података. Идеја о уградњи електронских чипова у пластичне картице уопште није нова; стара је колико и криптографија са јавним кључевима. Први патенти потичу од пре двадесетак година, док је масовна производња и примена интелигентних картица релативно новија.

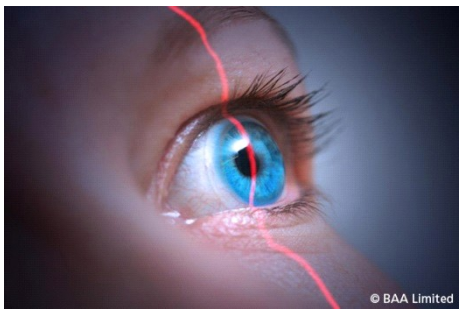
Последњих година највише корисника интелигентних картица налази се у оквиру државне администрације, телефонских оператора, банака, осигуравајућих друштава, а развој Интернета је отворио и нека друга тржишта.

На картици се могу налазити различити подаци, као што су: назив издавача, име власника, фотографија, рок важности. Језгро интелигентне картице чине програмабилни микропроцесор и одговарајуће меморије типа RAM, ROM и EPROM. Интелигентне картице комуницирају са спољним светом преко специјализованих улазно-излазних уређаја рачунара. Интелигентне картице знатно унапређују сигурносне механизме. Тајни кључ може бити записан на интелигентној картици, и може бити активиран само уз помоћ власника картице, како би се извршио одговарајући криптографски алгоритам.

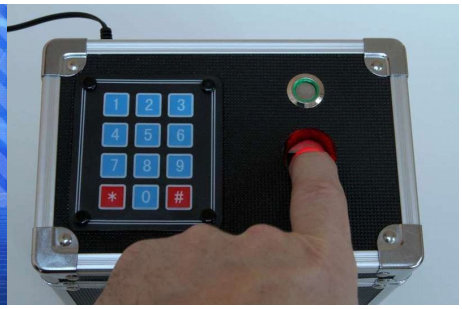
БИОМЕТРИЈСКИ СИГУРНОСНИ МЕХАНИЗМИ

Све шира примена интернет технологија у пословању доводи, нажалост, и до пораста криминала на Интернету, што захтева стално усавршавање заштитних механизама. Биометријски сигурносни механизми представљају посебно атракивну технологију заштите у којој се користе јединствене биолошке карактеристике људи, као што су отисак палца, боја глас аили изглед зенице - како би се идентификовао корисник.

На пример, помоћу камере се слика палца записује у шифрованом дигиталном облику и по потреби упоређује са сликом палца корисника који се представља систему.


© BAA Limited


PRT BIOMETRICS 08:17 08/09/2011


1 2 3
4 5 6
7 8 9
* 0 #