A Kriptográfia szabályzat bemutatása a Datatronic Kft.

dolgozói részére

2025. szeptember

Előadás menete

- Követelmények
- Szabályozás
  - Cél
  - Alapelvek
  - Kriptográfiai megoldások
  - Titkosító rendszerek
  - Eszközök
  - Titkosító kulcsok
  - Tanúsítványok
  - Pulbic Key Infrastructure - PKI
  - Kulcsokkezelése (eljárás)
- Kérdések

Cél

A Kriptográfiai szabályzat célja, hogy meghatározza a Datatronic Kft. számára:

- a kriptográfiai eljárások és eszközök kiválasztásának és alkalmazásának követelményeit és szempontjait;
- a PKI architektúra kialakításának követelményeit és szempontjait;
- a kriptográfiai kulcsok kezelésének szabályait és eljárásrendjét;
- az adattárolásra, illetve -továbbításra vonatkozó védelmi intézkedéseket;

Alapelvek

Kriptográfia alkalmazása esetén a legfontosabb alapelvek:

- ha egy információ el van rejtve, az még nem jelenti azt, hogy védve is van;
- ha egy információ el van rejtve, és védve is van, az nem jelenti azt, hogy nem hozzáférhető.

Ennek megfelelően meg kell fontolni kriptográfiai védelmi intézkedések alkalmazását minden olyan esetben, amikor az alábbi kritériumok bármelyikének biztosítása indokolt:

- **Bizalmasság** (az információ ne jusson illetéktelenek birtokába);
- **Sértetlenség** (az információ az illetékeshez teljességét és pontosságát megőrizve jusson el);
- **Letagadhatatlanság** (igazolható legyen az információ forrása – a forrás illetékessége vagy illetéktelensége).

Kriptográfiai megoldások

- Rejtjelezés/megfejtés (encryption/decryption);
- Elektronikus aláírások, időpecsétek (digital signature, time stamp);
- Hitelesítés (certification);
- Azonosítás (identification);
- Azonosító-hitelesítés (authentication);
- Jogosultságok kiosztása, tulajdonság birtoklás (authorization, attribute ownership);
- Hozzáférés szabályozás (access-control);
- Titokmegosztás, titokszétvágás (secret sharing/splitting)

Titkosító rendszerek

A titkosítási feladatok végrehajtásához különböző titkosító rendszerek állnak rendelkezésre a kulcsok száma alapján:

- szimmetrikus v. egykulcsú;
- aszimmetrikus v. két kulcsú v. nyilvános kulcsú;
- hibrid (a fenti kettőt ötvözi);

a használt műveletek szerint:

- helyettesítő;
- keverő;
- produkciós (összetett v. kompozíciós);

a nyílt szöveg feldolgozása szerint:

- blokktitkosítók;
- folyamtitkosítók.

Szimmetrikus titkosítás

A szimmetrikus típusú titkosítás ugyanazt az kulcsot (algoritmust) használja titkosításra és visszafejtésre egyaránt, ezért a feladónak és a címzettnek is vigyáznia kell rá, hogy titokban maradjon. Ezt a megoldást tehát olyan helyen érdemes alkalmazni, ahol a küldés (rejtjelezés) és a fogadás (visszafejtés) ugyanazon a helyen történik.
A szimmetrikus titkosításnak két fajtája különböztethető meg:
kétirányú – amikor szükség van a titkosított információ visszafejtésére, pl:

- fájlrendszer titkosítás;
- titkosítás adattároló rendszerekben;
- titkosítás mentőrendszerben, adattárolás céljából;

egyirányú – amikor az elrejtett információ visszafejtése nem szükséges (az információ titokban maradhat, titkosított változata (ún. lenyomata) elegendő pl. egyezőség bizonyítására), pl:

- tudás alapú azonosítás (pl. titkosított jelszó-tárolás);
- digitális aláírás készítés;

Engedélyezett szimmetrikus algoritmusok és kulcshossz értékek:

- AES algoritmusú 256 bites kulcshosszú
- AES algoritmusú 512 bites kulcshosszú

Engedélyezett hash függvények és kulcshossz értékek:

- SHA algoritmusú 256 bites kulcshosszú
- SHA algoritmusú 384 bites kulcshosszú
- SHA algoritmusú 512 bites kulcshosszú

Az engedélyezett titkosítási értékek és paraméterek (algoritmus, kulcshossz, hash függvények, stb.) meghatározása a CTO felelőssége

Aszimmetrikus kódolás

Az aszimmetrikus kriptográfiai rendszerek esetében a titkosító kulcs és a visszafejtő kulcs egyrészt különbözik egymástól, másrészt egy bizonyos titok ismerete nélkül, emberi léptékű időn belül nem számíthatók ki egymásból.
Az aszimmetrikus titkosítás bizalmas üzenetváltásokhoz, biztonságos kulcscserékhez, illetve – a szimmetrikus egyirányú titkosításhoz hasonlóan – digitális aláíráshoz alkalmazható. Hátránya, hogy – különösen hosszabb üzenetek esetében – rendkívül lassú.

Engedélyezett algoritmusok és kulcshossz értékek:
- RSA algoritmusú 2048 bites vagy hosszabb kulcshosszú
- ECC algoritmusú 224/256/384/512 bites kulcshosszú

Az engedélyezett titkosítási értékek és paraméterek (algoritmus, kulcshossz, hash függvények, stb.) meghatározása a CTO felelőssége

Hibrid titkosítás

A hibrid kriptográfiai rendszerek az aszimmetrikus eljárást csak a szimmetrikus kulcsok cseréjéhez alkalmazzák, az elrejtendő üzenetet szimmetrikus kulccsal titkosítják. Ilyen módon a hibrid kriptográfiai rendszerek egy szimmetrikus titkosító algoritmusból és egy kulcscsere protokollból állnak.

A hibrid kriptográfiai rendszerek a publikus hálózatokon keresztülhaladó adatforgalmak titkosítására, illetve digitális aláírásra használhatók hatékonyan.

Adatforgalom titkosítás

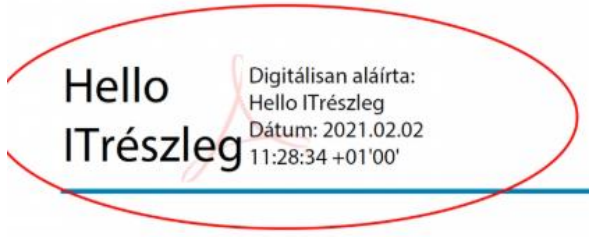
Engedélyezett protokollok:

- TLS verziója 1.2 vagy magasabb
- IPSec
- OpenVPN

Elektronikus aláírás

Az elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

- egyedi;
- másolhatatlan;
- a dokumentumtól elválaszthatatlan;
- az aláírót egyértelműen azonosítja;
- egyedülállóan az aláíróhoz köthető;
- a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumban tett – módosítás érzékelhető.



Eszközök

Az érzékeny információk védelmére az alábbi kriptográfiai eszközök használhatók:
Kriptográfiai kulcsok, amelyek az érzékeny információk elrejtését (rejtjelezését) szolgálják;
Tanúsítványok, amelyek az érzékeny információk birtokosát azonosítják és hitelesítik;

Kriptográfiai eszköz tárolók:

- token, amely hardveralapú titkosítást alkalmazó USB kulcs;

- Trusted Platform Modul (TPM), amely a számítógépekbe épített hardver alapú titkosítást alkalmazó integrált áramkör (chip);

- Hardver Security Module (HSM).

A Datatronic hálózatában használható kriptográfiai eszközök, ezek paramétereinek, valamint használati módjainak meghatározása a CTO felelőssége.

Kriptográfiai kulcsok

A titkosításhoz használt kulcsokat teljes életciklusuk alatt (létrehozás, kiosztás, archiválás, frissítés, visszavonás, megsemmisítés) védeni kell a jogosulatlan módosítástól, megtekintéstől és törléstől.

A kulcskezeléssel kapcsolatban az üzemeltetési feladatok megvalósítása a CTO felelőssége, a folyamat nem automatizált (eseti) biztonsági szerepköreinek feladatait (pl. biztonsági incidensek kivizsgálása, eszkaláció stb.) pedig a CISO végzi az ISMS Board jóváhagyásával.

A kulcsokhoz való hozzáférés, illetve kezelésük során biztosítani kell, hogy:

- a kriptográfiai kulcsokhoz csak az arra jogosultak férhessenek hozzá, akiknek ehhez a munkájuk során feltétlenül szükségük van;
- érvényesüljön a feladatok és felelősségek szétválasztásának elve;
- a kriptográfiai kulcsokhoz való hozzáférés naplózott legyen;
- a kriptográfiai kulcsok tárolása és továbbítása titkosítva történjen;
- a kriptográfiai kulcsok és a titkosításukhoz felhasznált jelszó továbbítása ne azonos kommunikációs csatornán történjen (;
- a kulcsok élettartama összhangban legyen a védett adatok érzékenységével és felhasználásának gyakoriságával;
- a titkosítási kulcsokról mindig készüljön biztonsági másolat váratlan események bekövetkezése esetére;
- életciklusuk végén a kulcsok megsemmisítése megfelelően megtörténjen (pl. az életciklus alapján akár automatikus megsemmisítést is lehet implementálni);
- kompromittálódás esetén megtörténjen a kulcs létrehozójának értesítése, valamint a kulcs megsemmisítése;

Tanúsítványok

Az SSL/TLS tanúsítványok olyan digitális dokumentumok, amelyeket az internetes biztonsági szolgáltatók állítanak ki a weboldalak számára a weboldal tulajdonosának hitelesítésére, valamint a biztonságos adatátvitel (titkosított csatorna) kialakítására.

A leggyakrabban használt SSL/TLS tanúsítványok a következők:

- Domain Validation (DV) SSL/TLS: a weboldal tulajdonjogát hitelesíti;
- Organization Validation (OV) SSL/TLS: a weboldal tulajdonjogát, valamint az oldalt birtokló szervezetet hitelesíti;
- Extended Validation (EV) SSL/TLS: a weboldal tulajdonjogát, a szervezetet és az üzleti tevékenységet is hitelesíti.

Tanúsítványok

Az SSL/TLS tanúsítványok több aldomainből álló domain-architektúra esetében is használhatók, ebben az esetben az alábbi típusok vehetők igénybe:

SAN (Subject Alternative Name) tanúsítványok:

- több alapdomain egyidejű védelmére;
- ritkán változtatott architektúra esetén;
- kevés számú, előre ismert nevű alap- és aldomainek esetén;

Wildcard (helyettesítő karakteres: pl. **.valami.hu*, ahol a csillag helyére bármely karakterkombináció behelyettesíthető) tanúsítványok:

- egyetlen alapdomain, de nagyszámú aldomain védelmére;
- előre nem ismert számú és nevű domainek esetén;

Multi-domain wildcard tanúsítványok:

- több alapdomainben nagyszámú aldomain esetében;
- több aldomainben előre nem ismert számú és nevű aldomain védelmére

Tanúsítványok

Amennyiben a Datatronic Kft. saját üzemeltetésű weboldalt kíván létrehozni, fentiek alapján az alábbi szabályokat kell alkalmazni:

- a weboldal működtetéséhez a wildcard tanúsítványok használatát lehetőség szerint el kell kerülni;
- amennyiben wildcard tanúsítványok használata nem kerülhető el:
  - mivel egy wildcard tanúsítvány minden esetben SPoF (Single Point of Failure), vagyis privát kulcsának kompromittálódása a teljes architektúra minden elemét magával rántja, beleértve a kapcsolódó háttérszervereket és adatbázisokat, ezért minden wildcard tanúsítvány privát kulcsát „4 szem elv” alkalmazásával kell tárolni (pl. a privát kulcsot kiolvasó folyamat service usere nem rendelkezhet írási joggal a kulcsot tároló mappában);
  - mivel a tanúsítványok lejártakor a tanúsítványokat minden érintett architektúra-elemen, a zökkenőmentes működés érdekében lehetőség szerint egyidejűleg kell megújítani, a wildcard tanúsítványok kezelésére standard change folyamato(ka)t kell kialakítani;
- mivel a lejárt SSL/TLS tanúsítványok már nem használhatók védelemre, az érintett weboldal automatikusan sérülékennyé válik, amelyet a böngésző jól láthatóan jelez „nem biztonságos” megjelöléssel; emiatt egyrészt korlátozódik az oldal elérése, másrészt az oldal negatív reputációs besorolást (negatív SEO - Search Engine Optimalization) kap, ami jelentős üzleti hátrányt okozhat; ezért az SSL/TLS tanúsítványok életciklus menedzsmentjére folyamatot kell kidolgozni és működtetni.

Tanúsítványok

Eszköztanúsítványok

Az eszköztanúsítványok két készülék egymáshoz csatlakozásakor szolgálnak kölcsönös azonosításra és hitelesítésre, valamint a tanúsítvány segítségével biztonságos adatátviteli csatornát is felépíthetnek egymás között. Mivel az eszköztanúsítványok alapvetően a belső hálózatokon történő azonosításra szolgálnak, ezeket a tanúsítványokat a Szervezet saját maga bocsátja ki, belső (privát) tanúsítvány-hitelesítő szerver (Certificate Authority – CA szerver) alkalmazásával. Ugyanakkor, mivel az eszköz-tanúsítvány csak magát a fizikai készüléket azonosítja, a felhasználóját nem, a Datatronic belső erőforrásainak külső hálózatokból való biztonságos eléréséhez csak indokolt esetben engedélyezhető.

Bármely, a Szervezet által felügyelt és működtetett publikus weboldalon, vagy az Internet felől közvetlenül elérhető alkalmazás-szolgáltatást nyújtó webszerveren self-signed (önaláírt), vagyis a Szervezet belső CA szervere által kibocsátott tanúsítvány használata **nem engedélyezett**.

Amennyiben eszköztanúsítvány használata engedélyezésre kerül, az alábbi követelményeknek kell teljesülniük:

- az eszköztanúsítványokról naprakész nyilvántartást kell vezetni, amely az alábbiakat kell, hogy tartalmazza:
  - mikor és hogyan (azaz milyen folyamatok és eljárások segítségével) kerültek kiadásra az eszköztanúsítványok;
  - a tanúsítványok lejárata;
  - tanúsítványgazda (életciklus-felelős).

A tanúsítványok nyilvántartásának meglétéért és naprakészségéért a CTO felelős

Tanúsítványok

Önaláírt tanúsítványok

Önaláírt tanúsítványok kizárólag a Datatronic belső informatikai rendszereiben használhatók, a belső IT infrastruktúra elemeinek azonosítására és védelmére.

A tanúsítvány- és kulcsgenerálást feljogosított személynek kell végeznie.

Tanúsítványok

Személyes tanúsítványok

A felhasználói tanúsítvány biztonságát a felhasználó privát kulcsának biztonsága határozza meg. Ennek megfelelően a belső PKI-n kívül:

- biztosítani kell, hogy a privát kulcshoz lehetőség szerint csak a kulcs felhasználója férhessen hozzá (pl. személyes használatú biztonsági tokenen, vagy a felhasználó mobil eszközébe épített biztonságos TPM chip alapú tárolóban létrehozva);
- a kulcsgeneráló folyamatnak véletlen kulcs értékeket kell létrehoznia, és biztosítania kell, hogy két felhasználó nem kaphasson azonos kulcsokat;
- a publikus és privát kulcspárok létrehozásakor erős (minimálisan nyolc karakter hosszú) passphrase-t kell használni. A kapott passphrase-t nem szabad másokkal megosztani;
- a privát kulcsot tartalmazó könyvtár megosztása nem engedélyezett;
- a tanúsítványhoz tartozó név (distinguished name) regisztrációja során biztosítani kell, hogy két felhasználót ne lehessen összekeverni.

Biztonsági token

A biztonsági token olyan fizikai vagy digitális eszköz, amely a többfaktoros hitelesítési (MFA) folyamatban az azonosításhoz és hitelesítéshez szükséges birtokolt kellék (kártya, usb kulcs, mobileszköz, rádiófrekvenenciás azonosító eszköz stb.), amely egy felhasználóról biztonsági információkat tartalmaz, és amelyet a rendszer ellenőrizhet.

A tokeneket leggyakrabban számítógépes hálózatokhoz való hozzáféréshez használják, de biztosíthatnak fizikai hozzáférést épületekhez, valamint elektronikus aláírásként is szolgálhatnak dokumentumokhoz.

Az azonosítási és hitelesítési folyamat kezdetén az eszköz véletlen számot generál, titkosítja és elküldi a hitelesítő szervernek a felhasználó hitelesítési információival. A szerver ezután egy titkosított választ küld vissza, amelyet csak az eszköz tud visszafejteni. Az eszközt minden hitelesítéshez újra felhasználják, így a hitelesítő szervernek nem kell felhasználónevet vagy jelszót tárolnia.

Biztonsági token

A biztonsági tokenek típusai:

Egyszer használható jelszó (One-time password – OTP). Az OTP lényege, hogy minden egyes használat után a hitelesítési szerver értesítést kap arról, hogy az OTP-t nem szabad újra felhasználni.

Leválasztott (disconnected) token. Az eszköz sem fizikailag, sem logikailag nem kapcsolódik az elérendő rendszer elemeihez, általában OTP-t vagy más hitelesítő adatokat generál. Pl. egy asztali alkalmazás, amely bejelentkezéshez szükséges szöveges üzenetet küld a mobiltelefonra, ilyen tokent generál.

Csatlakoztatott (connected) token. Olyan fizikai eszköz, amely visszafejthetetlenül titkosított formában (rendszerint hardveres titkosítással) tartalmazza az azonosítási és hitelesítési információkat, emiatt közvetlenül csatlakoztatni kell egy számítógéphez vagy érzékelőhöz (Pl. Yubikey, Gemalto USB kulcsok).

Érintés nélküli token. A csatlakoztatott tokenhez hasonlóan tárolja az azonosítási és hitelesítési információkat, de fizikai kapcsolatot nem, csak logikai kapcsolatot létesít a hozzáférés engedélyezésére szolgáló számítógéppel vagy berendezéssel (pl. Bluetooth kommunikációs protokoll segítségével).

Egyszeri bejelentkezési (SSO) szoftverjogkivonatok. Az egyszeri bejelentkezési szoftver tokenek digitális információkat tárolnak, például felhasználónevet vagy jelszót. Lehetővé teszik a több számítógépes rendszert és több hálózati szolgáltatást használó felhasználók számára, hogy minden rendszerbe bejelentkezzenek anélkül, hogy több felhasználónevet és jelszót kellene megjegyezniük.

Programozható token. A programozható biztonsági token ismételten létrehoz egy egyedi kódot, amely egy meghatározott időtartamig, gyakran 30 másodpercig érvényes. Például az Amazon Web Services Security Token Service egy olyan alkalmazás, amely 2FA kódokat generál, amelyek az információs technológiai adminisztrátorok számára szükségesek bizonyos AWS felhő-erőforrások eléréséhez.

Biztonsági token

Az alábbi szabályokat kell betartani:

Többfaktoros authentikáció esetében a bejelentkezésre használt eszköznek és a biztonsági tokennek fizikailag el kell különülnie egymástól (a laptop és a laptopba épített TPM chip alapú tárolóban elhelyezett authentikációs információ – pl. tanúsítvány – nem tekinthető teljes értékű többfaktoros hitelesítési megoldásnak – mivel pl. a laptop eltulajdonítása esetén a biztonsági token is a támadó birtokába kerül.

Érintés nélküli token alkalmazásának bevezetése előtt eseti kockázatelemzést kell végrehajtani, és az abban feltárt kockázati eseményeket (fenyegetéseket) át kell vezetni az éves rendszeres kockázatelemzés során vizsgált lehetséges fenyegetések közé.

Public Key Infrastructure (PKI)

A PKI (Nyilvános Kulcsú Infrastruktúra) olyan keretrendszer, amely algoritmusokat, folyamatokat, szabályozásokat és technológiákat integrál, hogy bármely hálózaton – függetlenül annak méretétől vagy tulajdonosától - biztonságos elektronikus adatátvitelt tegyen lehetővé.

A PKI aszimmetrikus titkosításra épül, amely két kriptográfiai kulcs használatán alapul: egy nyilvánosan elérhető nyilvános kulcson és egy privát kulcson, amelyet a felhasználó vagy a szervezet rejtve tart. Ezeket a kulcsokat párhuzamosan használják kriptográfiai műveletek (titkosítás, visszafejtés) végrehajtására, valamint digitális aláírások és digitális tanúsítványok előállítására.

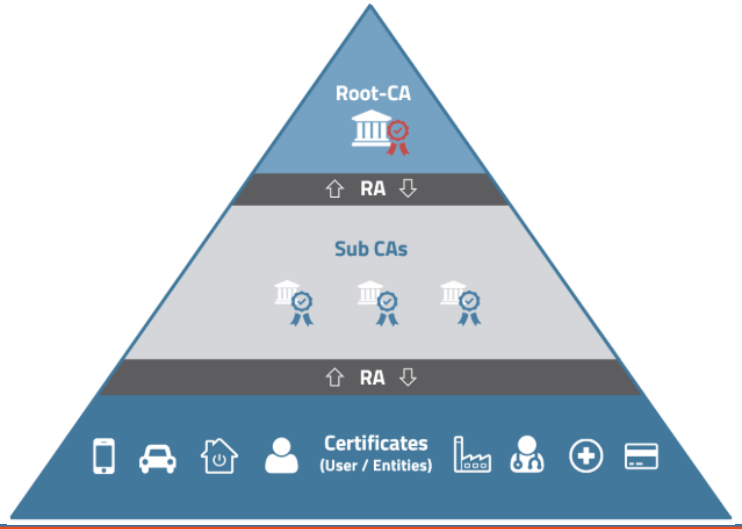
A Datatronic PKI architektúrájának tervezése, kialakítása, működtetése és karbantartása a CTO felelőssége.

Public Key Infrastructure (PKI)

A PKI összetevői

CA (Certification Authority – Hitelesítés Szolgáltató).
Funkciói:

- RSA kulcspárok generálása;
- X.509 tanúsítványok kibocsátása (a CA által aláírva);
- nyilvános kulcsok személyekhez kötése;
- tanúsítvány visszavonási listák generálása (Certificate Revication List - CRL);
- adatbázisok és névtárak kezelése;
- master kulcsok kezelése;



RA (Registration Authority).
Funkciói:

- felhasználó azonosító generálása;
- felhasználó kulcs kérése a CA-tól;
- felhasználó kulcs fogadása a CA-tól;
- felhasználó kulcs eltárolása (smart-kártyán vagy PKCS#12 kulcs fájlban);
- tanúsítvány visszavonás kérése a CA-tól;
- felhasználó kulcs megújítás/frissítés;
- felhasználó kulcs-visszaállítás;
- felhasználó törlés;
- felhasználó policy menedzsment;
- eseménynaplózás;
- policy fájl-exportálások;
- felhasználó tanúsítványok kérelme;
- kérelmek visszavonása;
- tömeges kulcs és tanúsítvány kezeléssel kapcsolatos műveletek batch üzemmódú kezelése;
- smart-kártya kibocsátása, menedzsmentje.

Public Key Infrastructure (PKI)

A PKI összetevői

User Agent (PKI kliens). Funkciói:

- digitális alírás képzés;
- kódolás, dekódolás;
- hitelesítési eljárások;
- tanúsítvány kérelmek;
- policy management révén, megfelelő jogosultság birtokában:
  - kulcs megújítás kérelmek;
  - visszavonási kérelmek;
  - a helyi RSA kulcs pár generálása, smart kártya kibocsátás.

Tanúsítványtár: címtár, melyben a CA a kibocsátott tanúsítványokat, illetve visszavonási listákat tárolja és a nyilvánosság számára elérhetővé teszi;

Visszavonási Listák:

- Tanúsítvány visszavonási lista (Certificate Revication List - CRL):
  - ha lejár a tanúsítvány érvényességi ideje;
  - ha a tanúsítványt birtokló felhasználó titkos kulcsa kompromittálódott;
  - ha a tanúsítványt kiállító CA titkos kulcsa kompromittálódott;
  - ha a regisztrált felhasználó törlését kéri akár az RA, akár a CA nyilvántartásából;
- Szervezeti visszavonási lista (Certification Authority Revocation List – CARL), más CA-k részére kibocsátott tanúsítványok visszavonására;
- Delta visszavonási lista (dCRL), a legutóbbi, vagy azt megelőző CRL-ek közzététele óta érvényüket vesztett tanúsítványok visszavonására;

Tanúsítvány szabályzat (Certificate Policy), amely a CA, a tanúsítvány használója és a tanúsítványhoz regisztrált felhasználó jogait és egymással szembeni kötelezettségeit rögzítő dokumentum.

Public Key Infrastructure

A Datatronic belső PKI infrastruktúrájának alábbi elemei a legsérülékenyebbek:

- **CA és RA szerverek;**
- **CA szerver master (root certificate kiállító) privát kulcsa;**
- **digitális tanúsítványok továbbításának kommunikációs útvonalai;**
- **az IT infrastruktúra elemek tanúsítványtárában tárolt tanúsítványok privát kulcsai és hitelesítő adatai.**

PKI védelmi intézkedések

A PKI infrastruktúrában szisztematikus, lehetőség szerint automatizált folyamatot (Systematic Certificate Lifetime Management) kell kialakítani a tanúsítványok kezelésére azok teljes életciklusa (igénylés, kibocsátás, megújítás, visszavonás során, amely meghatározza a kulcs-rotációs folyamatokat és eljárásokat is.

Tanúsítványkibocsátásra lehetőség szerint önálló, a belső hálózatban működő alkalmazás-, web- és adatbázis-kiszolgálóktól elkülönített hálózati szegmensben elhelyezett Certificate Authority (CA) szervert kell üzemben tartani. Ugyanebben a szegmensben kell elhelyezni a regisztrációs szervert (RA) is.

A Datatronic minden saját tulajdonú tanúsítványát nyilvántartásba kell venni és naprakészen kell tartani, az alábbi adattartalommal:

- tanúsítvány neve;
- tanúsítvány kibocsátó;
- használat helye;
- tanúsítványgazda;
- kulcshossz;
- algoritmus;
- lejárat.

PKI védelmi intézkedések

Biztosítani kell a regisztrációs és a tanúsítványkezelő szerverek, valamint privát kulcsaik fizikai (pl. adatközponti üzemeltetés) és logikai (titkosított tárolás) védelmét egyaránt; a kulcsokat a lehető legkevesebb helyen szabad csak tárolni.

A PKI infrastruktúra szerverekhez hozzáférők számát korlátozni kell, a hozzáférőkről nyilvántartást kell vezetni (pl. speciális global security csoport létrehozásával az Active Directoryban).

A PKI infrastruktúra szerverek és a kliensek között csak szabványos protokollok használata engedélyezett (LDAP, PKIX-CMP/PKCS). A tanúsítvány létrehozása során biztosítani kell a sértetlenséget, különösen a CA és az RA között.

A szerver elmentett privát kulcsának felhasználása előtt ellenőrizni kell a kulcs sértetlenségét (pl. a kulcs hash lenyomatának vizsgálatával).

A CA privát kulcsának kompromittálódása esetén az összes aláíró tanúsítványt vissza kell vonni.

Valamely szerver privát kulcsának kompromittálódása esetén:

- azonnal el kell végezni a kulcsok visszavonását;
- új kulcspárt és kapcsolódó tanúsítványt kell beszerezni a CA-tól;
- a kompromittálódott privát kulcsokat meg kell semmisíteni;
- a megsemmisítés tényét dokumentálni kell.

PKI védelmi intézkedések

A tanúsítványoknak és kulcsoknak korlátozott idejű érvényességgel kell rendelkezniük. Az érvényesség idejét a kompromittálódás biztonsági kockázata, a jogosultságmódosítási igények, valamint a technikai és üzemeltetési körülmények határozzák meg.

Kompromittálódás esetén lehetőséget kell biztosítani a kulcsok cseréjére.

A PKI infrastruktúrában lehetőséget kell biztosítani a titkosításra használt kulcsok helyreállítására, illetve a titkosított információ megfejtésére. A kulcs-helyreállítási eljárást dokumentálni kell.

A tanúsítványellenőrzési folyamat során meg kell vizsgálni, hogy a tanúsítvány nem szerepel-e a visszavonási listán (revocation list).

A CA szervernek fel kell tennie a felhasználó lejárt tanúsítványát a visszavonási listára.

Ezen nyilvántartások meglétéért és naprakészen tartásáért a CTO felelős.

Kriptográfiai kulcsok kezelése

Eljárás

A kulcsok és tanúsítványok igénylését a felhasználók, illetve szervertanúsítvány esetén az IT támogató csoport kezdeményezheti a Jogosultságkezelési Szabályzatban leírt jogosultságigénylési folyamat szerint.

Külső felek igénylését a Datatronic kapcsolattartó munkatársa kezdeményezi, szintén a jogosultságigénylési folyamat szerint.

A tanúsítvány csak akkor rendelhető személyhez és adható át számára, ha a felhasználási feltételeket megismerte és elfogadja.

A CTO hagyja jóvá a kulcsok és tanúsítványok használatára jogosultak körét. A CTO felelőssége továbbá, hogy a kiadott engedélyeket naprakészen nyilvántartsa. A nyilvántartást elérhetővé kell tennie a CISO számára.

A kulcsot, illetve tanúsítványt azok felhasználójának személyesen kell átvennie, vagy a kulcsot és a hozzá tartozó jelszót külön csatornán kell eljuttatni a felhasználónak.

A kibocsátott privát kulcsot és tanúsítványt az IT támogató csoport telepíti.

Az IT szolgáltató által üzemeltetett szerveren a tanúsítványt az IT szolgáltató telepíti.

A hozzáférés funkcionális működését a felhasználónak tesztelnie kell.

Kriptográfiai kulcsok kezelése

Eljárás

A kulcsért, illetve a tanúsítványért felelős személynek az adott helyzetben elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze az illetéktelen felhasználást.

A privát kulcsot védő jelszót a felhasználó nem hozhatja más tudomására.

A felhasználó privát kulcsát csak olyan célokra és olyan alkalmazásokkal használhatja, melyek a kiadott engedélyben szerepelnek.

A kriptográfiai kulcs átadásakor az IT támogató csoportnak be kell állítania, hogy a felhasználó privát kulcsát tartalmazó könyvtárhoz (amennyiben az másképp nem, csak az eszközön lokálisan tárolható) kizárólag a felhasználó férhessen hozzá.

Az IT csoportnak a privát kulcs kiolvashatóságát (export) minden esetben tiltaniuk kell, illetve amennyiben a kulcstárolásra speciális eszköz (pl. TPM chip alapú tároló, USB token, smartcard stb.) kerül használatba, az eszköznek biztosítania kell, hogy a magánkulcs az eszközről ne legyen kiolvasható

Kriptográfiai kulcsok kezelése

Eljárás

A kriptográfiai kulcs átadásakor az IT támogató csoportnak be kell állítania, hogy a felhasználó privát kulcsát tartalmazó könyvtárhoz (amennyiben az másképp nem, csak az eszközön lokálisan tárolható) kizárólag a felhasználó férhessen hozzá.

Az IT csoportnak a privát kulcs kiolvashatóságát (export) minden esetben tiltaniuk kell, illetve amennyiben a kulcstárolásra speciális eszköz (pl. TPM chip alapú tároló, USB token, smartcard stb.) kerül használatba, az eszköznek biztosítania kell, hogy a magánkulcs az eszközről ne legyen kiolvasható.

A tanúsítvány használatának megszűnése után:

- a privát kulcs nem archiválható;
- a tanúsítványt viszont archiválni kell a korábbi felhasználás azonosíthatósága és ellenőrizhetősége érdekében.

Kriptográfiai kulcsok kezelése

Eljárás

Amennyiben a felhasználó tanúsítványát (smartcard-ját, tokenét vagy mobil eszközét) eltulajdonították, elvesztette vagy megsérült, akkor:

- a felhasználónak haladéktalanul be kell jelentenie a Service Desk – Jira rendszerben vagy a CTO-nak közvetlenül és információbiztonsági incidenskezelési folyamatot kell indítani;
- a CA-ban vissza kell vonni a felhasználó tanúsítványait és kulcsait;
- új kulcspárt és tanúsítványt kell létrehozni a felhasználónak, illetve érintettség esetén új kártyát (tokent) kell kiadni;
- az új kártya (token) használata előtt meg kell bizonyosodni róla, hogy a korábbi kulcsok és tanúsítványok törlése megtörtént.

A tanúsítványtár és kulcsnyilvántartás naprakészen tartása a CTO felelőssége.

Kriptográfiai kulcsok kezelése

Eljárás

A tanúsítványkezeléssel kapcsolatos folyamatokat definiálni kell a PKI üzemeltetési dokumentációjában. Az üzemeltetési leírásnak a következőkre kell részletesen kitérnie:

- erős kriptográfiai kulcsok generálása;
- kriptográfiai kulcsok biztonságos kiosztása;
- kriptográfiai kulcsok visszavonása (revocation) és érvényesítés (validation);
- kriptográfiai kulcsok helyreállítása;
- kriptográfiai kulcsok megújítása (renewal) az érvényesség lejártát megelőzően.

Az alkalmazásokhoz tartozó megbízható domain-ek (trusted domains) bővítéséhez, módosításához, törléséhez változáskezelési folyamatot kell indítani.

Adattitkosítás

Eljárás

Nem nyilvános adatokat csak titkosítva szabad a notebookokra, adathordozókra másolni, amennyiben az eszközt a felhasználó a Datatronic üzemeltetési hálózatán kívül is használja.

Érzékeny adatokat munkaállomásokon, notebookokon, szervereken és külső adathordozókon egyaránt titkosítva kell tárolni.

A hordozható eszközök adathordozóin fájlszintű titkosítást kell alkalmazni érzékeny besorolású adatok tárolása esetén. A hozzáféréshez minimálisan jelszó szükséges.

A védelmi intézkedések kialakítása és bevezetése a CTO, az intézkedések betartásának rendszeres ellenőrzése a CISO feladata.

Adatok átvitele

Eljárás

Minden üzenethez egyedi szimmetrikus kulcsot kell generálni, a használat után a kulcsot törölni kell.

Csak korlátozott felhasználói csoportok továbbíthatnak – megfelelő naplózás mellett – érzékeny adatokat külső eszközök (külső merevlemez, notebook) felé.

Titkosítást kell alkalmazni adatátvitel során, amennyiben nyilvános hálózatot érint a kommunikáció. Nyilvános hálózatnak minősül pl. az Internet, illetve az olyan (al)hálózat, amely mindenki által elérhető (pl. DMZ).

Vezetéknélküli hálózatok (például: Wi-Fi, GPRS, RF) forgalmát titkosítani szükséges.

Authentikációs adatokat (pl. jelszó) a Datatronic informatikai hálózatán belül is csak titkosított adatcsatornán keresztül szabad továbbítani.

Lehetőség szerint titkosított adatcsatornát kell használni a „trusted” kapcsolatban lévő rendszerek kommunikációjában is.

Az érzékeny információ külön titkosított fájlban is csatolható a levélhez, ilyenkor csak abban az esetben van szükség a levél titkosítására, ha a levéltörzs vagy a tárgy is tartalmaz érzékeny információkat. Ezen titkosítás esetében a csatolmányhoz tartozó jelszót külön csatornán kell továbbítani. Illetve a jelszónak meg kell felelnie a Szervezet jelszó követelményeinek.

Külső elérés esetén csatornatitkosítást kell alkalmazni a rendszerekhez/alkalmazásokhoz történő adminisztratív és üzemeltetői hozzáférések esetén.

A védelmi intézkedések kialakítása, bevezetése és folyamatos működtetése a CTO, az intézkedések betartásának rendszeres ellenőrzése a CISO feladata.

Kérdések

DATATRONIC

TrustaaS
IT RISK MANAGEMENT

Köszönöm a figyelmet!