**Authentikációs rendszer korszerűsítése – műszaki specifikáció**

**Koncepció:**

Meglévő hardver alapú erős authentikácós megoldás kiváltása, korszerűbb, biztonságosabb, hard-token és soft-token alapú megoldásra, HA kiépítésben. A kiépítés fizikai, gyártói appliance alapú elsődlegesen, HA párja VMware vagy Hyper-V környezetbe egyaránt telepíthető legyen. Három év teljes körű gyártói garancia elvárás, a tokenek minimum 5 éves lejárattal rendelkezzenek.

**Műszaki követelmények:**

* VMware és Hyper-V virtuális környezet támogatása
* hardveres és szoftveres OTP (One Time Password) alapú token-ek
* LDAP alapú külső authentikációs források használata
* SMS és email alapú OTP küldési lehetőség
* self-service portál
* a későbbiek során a költséghatékonyság, és felhasználói kényelem érdekében kockázat elemzésen alapuló authentikáció mint lehetőség legyen biztosítva
* elsődlegesen gyári appliance kivitelű telepítés (szoftveresen csak a HA pár legyen telepíthető)
* a hardveres/szoftveres token nem lehet OATH szabványú
* felhő alapú hybrid kiegészítő megoldással legyen integrálható
* a hard-token legyen képes tanúsítvány tárolására, OTP kijelzésére és USB csatlakozófelülete legyen.

**Tanúsítvány-tárolással kapcsolatos követelmények:**

* a tanúsítvány-generálás Microsoft CA-val történik,
* a hordozóeszközre legalább 2 X.509-es tanúsítványt el kell tudni helyezni, egyet digitális aláíráshoz, egyet a belépési folyamatok számára
* tanúsítvány egyrészt generáljon úgy az eszköz, hogy a tanúsítvány privát része ne hagyja el a hordozót, másrészt legyen lehetőség máshol generált fájlban tárolt tanúsítvány elhelyezésére.
* Támogatnia kell mind a PKCS #11 specifikációit, mind a Microsoft CryptoAPI architektúráját, SSL és IPsec/IKE Pro szabványokat, RSA 1024-bit, 3DES, SHA1 biztonsági algoritmusokat.
* A tanúsítvány elérése csak PIN-kód megadása után legyen lehetséges.
* A PIN-kód megváltoztatását a felhasználó el tudja végezni.
* A tanúsítvány megváltoztatását, törlését adminisztratív joghoz kell kötni.

**Felhasználói címtártámogatással kapcsolatos követelmények:**

* Párhuzamosan több (minimum 2) a felhasználói körben eltérő címtár használata.
* Következő Címtárak támogatása: Microsoft AD, OpenLDAP.

**Elvárt szolgáltatások a projektben:**

* Tervezés
* Alaptelepítés
* HA kialakítás
* egyidejű OpenLDAP és Microsoft AD integráció
* Paraméterezés
* Oktatás
* Dokumentálás
* Tesztelés
* Projektvezetés

**Mintakonfiguráció:**

|  |  |  |
| --- | --- | --- |
| Cikkszám | Megnevezés | Mennyiség |
| RSA-80010500INT | RSA SecurID AM8 Intel Appliance 130  Hardware (includes Advanced Hardware  Replacement for Years 1-3) | 1 db |
| AUT0000750B8 | SID Access Base Perp from 505 - 750u | 550 db |
| AUT0000750BE1-8 | SID Access Base EnhMnt 1Mo | 19800 db |
| SID800-6-60-60-A | SID800-6-60-60 per user qtys 255-750 | 350 db |
| SID820-8-60-60-A | RSA SecurID Software Token Seeds (60  month) per User for qty's between 10 -  250 | 200 db |
| Telepítés | Tervezés, HA design, integráció, implementáció, dokumentálás (rendszerterv, rendszerbiztonsági terv, felhasználói és üzemeltetői dokumentációk), tesztelés, oktatás, projektvezetés (mérnöknap) | ………nap |