**Տ Ե Խ Ն Ի Կ Ա Կ Ա Ն Բ Ն ՈՒ Թ Ա Գ Ի Ր**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Չ/Հ | **Անվանումը** | **Տեխնիկական բնութագիրը** | **Չափման միավորը** | **Քանակը** | **Միավորի նախահաշվային գինը** | **Մատակարարման վայրը** | **Մատակարար ման ժամկետը** |
| 1 | Ամպային տեխնոլոգիաների վրա հիմնված բազմաֆունկցիոնալ վավերացման և մուտքի վերահսկման համակարգ | **VIP Service B2E, Initial Cloud Service Subscription 1y 500 users with support**  Թվային բանալիների ամպային համակարգ 1 տարի 500 օգտվողի համար ժամկետով ներառյալ սպասարկումը  Պետք է համատեղելի լինի գործող համակարգի հետ։  Պետք է ապահովի ամպային տեխնոլոգիաների վրա հիմնված բազմաֆունկցիոնալ վավերացումը մուտքի վերահսկման համար  Լուծումը պետք է իրականացվի մեկ մուտքի (SSO) գործողությունների գործառույթները, հուսալի վավերացմամբ  Պետք է ապահովի մուտքի վերահսկում և օգտագործողի կառավարում | հատ | 500 | 21800 | ՀՀ, ք․ Երևան, Աբովյան 27  3-րդ հարկ | Պայմանագիրն ուժի մեջ մտնելու օրվանից 20 օրվա ընթացքում |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Հիմնական հատկանիշները  Արտաքին կամ ներքին ծառայություն տեղադրման հնարավորություն  Դիմումների առաջադեմ կատալոգ, SAML կամ վեբ օգտագործող միացումներ ստեղծելու համար պարզ ինտերֆեյս՝ գրեթե ցանկացած ամպի կամ ներքին վեբ հավելվածին աջակցելու համար  Ղեկավարման միասնական կետը պետք է ապահովի պլատֆորմներում վավերացման քաղաքականություն կիրառելու համար (պատուհան / UNIX, VPN, MS IIS, MS ADFS, Citrix NetScaler, Office365, Salesforce, Box, Dropbox և այլն)  Ներկառուցված աջակցություն միանգամյա գաղտնաբառերի վրա՝ հիմնված անվտանգ վավերացման տեխնոլոգիայի և թվային հավաստագրերի հիման վրա (PKI)  Ներկառուցված օգտագործողների գրացուցակ` սպասարկման գործառույթների իրականացման համար (գրանցում, գաղտնաբառի կառավարում և այլն), |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | ինչպես նաև նույնականացման  տվյալների ամենատարածված աղբյուրների ստանդարտների հիման վրա ինտեգրումը:  Բջջային կենտրոնացված ճարտարապետություն, վերացնում է շրջանցելու մուտքը և պաշտպանում բջջային սարքերից ներբեռնված տվյալները:  Անվտանգությունը   1. Ընկերության տեղեկատվության պաշտպանություն 2. Միայն սերտիֆիկացված օգտվողներ 3. Հասանելիություն դեպի ֆայլեր, ծրագրեր, էլ. փոստ 4. Օգտագործելով ժամանակակից ծրագրեր 5. Հաշվետվություն, աուդիտ և մոնիտորինգ   Համակարգը պետք է նախագծված լինի հուսալի վավերացման համար` բանկային, առևտրային գործարքների համար։ |  |  |  |  |  |