ДОГОВОР

Днес,.....2020 г., в гр. София, между:

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ" АД, ЕИК: 831641791, със седалище и адрес на управление: гр. София 1504, район „Оборище", ул. „Панайот Волов"№ 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, в качеството му на системен интегратор по чл. 7с от Закона за електронното управление и публичен възложител на обществени поръчки по смисъла на § 45, ал. 1 от Преходните и заключителни разпоредби към Закона за изменение и допълнение на Закона за електронното управление, наричано по-долу за краткост **ВЪЗЛОЖИТЕЛ**, от една страна,

и

„СИЕЛА НОРМА" АД, със седалище и адрес на управление гр. София, п.к. 1510 район „Подуяне", бул. „Владимир Вазов" № 9, ЕИК/БУЛСТАТ: 130199580, представлявано от Веселин Тодоров – изпълнителен директор, наричан по-нататък за краткост **„ИЗПЪЛНИТЕЛ"**

(**ВЪЗЛОЖИТЕЛЯТ** и **ИЗПЪЛНИТЕЛЯТ** наричани заедно „Страните", а всеки от тях поотделно „Страна")

на основание чл. 112 от Закона за обществените поръчки (ЗОП), във връзка с чл. 69 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП), след проведена „открита" процедура за възлагане на обществена поръчка с предмет **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите"**

и въз основа на Решение № 51-00-30-19/31.07.2020 г. на изпълнителния директор на „Информационно обслужване" АД за определяне на изпълнител на обществена поръчка по обособена позиция № 8 с предмет: „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията" (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, се сключи този договор (**„Договора/Договорът"**) за възлагане на обществена поръчка.

Страните се споразумяха за следното:

I. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. (1) **ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** приема срещу възнаграждение да осъществи следните дейности:

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер" или „доставките"), подробно описан по вид, количество и технически характеристики в Техническата спецификация на **ВЪЗЛОЖИТЕЛЯ** с предмет: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите" – Приложение № 1 (наричана по-нататък „Техническа спецификация"), Приложение към нея, относимо към обособена позиция № 8 с предмет „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията" - Приложение № 1.8 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* и Техническото предложение на **ИЗПЪЛНИТЕЛЯ** по обособена позиция № 8 – Приложение № 2.8 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, представляващи неразделна част от настоящия договор.

2. гаранционно обслужване на доставения софтуер по т. 1 (наричано алтернативно „гаранция и поддръжка"), осигурено в рамките на срока по чл. 4, ал. 3 в съответствие с предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) Доставката на софтуера по ал. 1, т. 1 се извършва от **ИЗПЪЛНИТЕЛЯ** въз основа на писмена заявка до **ИЗПЪЛНИТЕЛЯ**, отправена чрез адреса за кореспонденция на хартиен носител, или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на **ВЪЗЛОЖИТЕЛЯ** или упълномощен негов представител, съгласно клаузите на този договор. В писмената заявка се посочват:

1. Вид и обем на софтуера, който следва да бъде доставен;

2. Място на доставка;

3. Срок на доставка, съобразен със сроковете и условията на доставка по настоящия договор.

4. Друга информация по преценка на **ВЪЗЛОЖИТЕЛЯ**, относима към изпълнението на договора.

II. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 2. (1) Общата цена по договора е в размер на 1 458 774.00 лева (един милион четиристотин петдесет и осем хиляди седемстотин седемдесет и четири лева и нула стотинки) без ДДС, съгласно Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.8 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, неразделна част от настоящия договор.

(2) **ВЪЗЛОЖИТЕЛЯТ** заплаща на **ИЗПЪЛНИТЕЛЯ** цената за изпълнената доставка съобразно цените на доставения и приет софтуер, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.8 към настоящия договор (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*.

(3) В цените по ал. 2, съответно в общата цена по ал. 1, са включени всички разходи на **ИЗПЪЛНИТЕЛЯ** по изпълнението на договора, като **ВЪЗЛОЖИТЕЛЯТ** не дължи заплащането на каквито и да е други разноски по договора.

(4) Цените по ал. 2, съответно общата цена по ал. 1, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.8 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* са крайни и не могат да бъдат променяни за срока на договора, освен в случаите, когато промяната е в полза на **ВЪЗЛОЖИТЕЛЯ,** както и при спазване на реда и условията на ЗОП.

Чл. 3.(1) Плащането се извършва в срок до 30 (тридесет) дни след представяне на следните документи:

1. Двустранно подписан приемо-предавателен протокол за извършена доставка по чл. 6, ал. 1; съответно чл. 6, ал. 2, когато е приложимо.

2. Оригинална фактура, предоставена от **ИЗПЪЛНИТЕЛЯ**, която съдържа подробна разбивка по единични цени, по услуги и видове за всеки един компонент, съдържащ се в доставения софтуер.

(2) Плащането се спира, когато **ИЗПЪЛНИТЕЛЯТ** бъде уведомен, че фактурата му не може да бъде платена, тъй като сумата не е дължима поради липсващи и/или некоректни придружителни документи или наличие на доказателства, че разходът е неправомерен. В този случай, **ИЗПЪЛНИТЕЛЯТ** трябва да даде разяснения, да направи изменения или представи допълнителна информация в срок до 3 (три) работни дни, след като бъде уведомен за това. В този случай срокът за извършване на плащане към **ИЗПЪЛНИТЕЛЯ** започва да тече от датата на която **ВЪЗЛОЖИТЕЛЯТ** получи правилно оформена фактура и/или поисканите разяснения, корекции и/или допълнителна информация.

(3) Плащанията се извършват от **ВЪЗЛОЖИТЕЛЯ** в български левове, с платежно нареждане по банкова сметка, посочена от **ИЗПЪЛНИТЕЛЯ**, както следва:

Банка: УниКредит Булбанк

IBAN: BG86 UNCR 9660 1060 7110 10

BIC: UNCRBGSF

(4) **ИЗПЪЛНИТЕЛЯТ** е длъжен да уведомява писмено **ВЪЗЛОЖИТЕЛЯ** за всички последващи промени по ал. 3 в срок до 3 (три) дни, считано от момента на промяната. В случай че **ИЗПЪЛНИТЕЛЯТ** не уведоми **ВЪЗЛОЖИТЕЛЯ** в този срок, счита се, че плащанията са надлежно извършени.

(5) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, **ВЪЗЛОЖИТЕЛЯТ** извършва окончателно плащане към него, след като бъдат представени доказателства, че

ИЗПЪЛНИТЕЛЯТ е заплатил на подизпълнителя/подизпълнителите за изпълнените от тях работи, които са приети по реда на раздел IV и са спазени условията на раздел IXа от настоящия договор.

III. СРОК И МЯСТО ЗА ИЗПЪЛНЕНИЕ

Чл. 4. (1) Договорът влиза в сила от датата на подписването му от двете страни и действието му се прекратява с изтичането на срока на гаранционното обслужване, посочен в ал. 3. Датата на подписване е датата, посочена в деловодния номер на **ВЪЗЛОЖИТЕЛЯ**, поставен на стр. 1 от настоящия договор.

(2) Срокът на извършване на доставката на софтуера е 10 (десет) календарни дни *(до 80 календарни дни съгласно изискванията на документацията за обществената поръчка по съответната обособена позиция)* от получаване на писмената заявка по чл. 1, ал. 2 от **ВЪЗЛОЖИТЕЛЯ**.

(3) Срокът на гаранционно обслужване на доставения софтуер е 5 години *(минимум 5 (пет) години съгласно изискванията на документацията за обществената поръчка по съответната обособена позиция)* и започва да тече от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.

Чл. 5. (1) Мястото на извършване на доставката е на територията на гр. София, като **ВЪЗЛОЖИТЕЛЯТ** ще посочи в писмената заявка по чл. 1, ал. 2 конкретния адрес на извършване на доставката.

(2) Гаранционното обслужване ще се извършва по местонахождението на доставения и инсталиран софтуер.

IV. УСЛОВИЯ НА ДОСТАВКА. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО

Чл. 6. (1) Приемането на всяка конкретна доставка на софтуера се удостоверява с двустранен приемо-предавателен протокол, който се подписва от упълномощените представители на страните по договора. При извършване на доставката на софтуер, **ИЗПЪЛНИТЕЛЯТ** представя на **ВЪЗЛОЖИТЕЛЯ** необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера. („**Приемо-предавателен протокол за доставка на софтуер**").

(2) При констатиране на явни недостатъци, повреди, дефекти, липси, и/или несъответствия на доставения софтуер с Техническата спецификация – Приложение № 1, Приложение № 1.8 към нея (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* или Техническото предложение – Приложение № 2.8 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* при извършване на прегледа по ал. 2, **ВЪЗЛОЖИТЕЛЯТ** има

право да откаже да подпише съответния приемо-предавателен протокол. В тези случаи страните подписват двустранен констативен протокол, в който се описват констатираните недостатъци, повреди, дефекти, липси и/или несъответствия и се посочва срокът, в който същите да бъдат отстранени („**Констативен протокол за липса на съответствие**"). След отстраняването им страните подписват двустранен приемо-предавателен протокол по реда и условията на ал. 1 за приемане на доставката.

(3) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, работата на подизпълнителя/подизпълнителите се приема от **ВЪЗЛОЖИТЕЛЯ** в присъствието на **ИЗПЪЛНИТЕЛЯ** и подизпълнителя/подизпълнителите.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ ПО ДОГОВОРА

Чл. 7. Изброяването на конкретни права и задължения на страните в този раздел от договора е неизчерпателно и не засяга действието на други клаузи от договора или от приложимото право, предвиждащи права и/или задължения на която и да е от страните.

Чл. 8. ВЪЗЛОЖИТЕЛЯТ има право да:

1. изисква от **ИЗПЪЛНИТЕЛЯ** да получи изпълнение съгласно условията на настоящия договор и приложенията към него;

2. извършва проверка във всеки момент от изпълнението на договора относно качество, обем, стадий на изпълнение, технически параметри без с това да пречи на оперативната дейност на **ИЗПЪЛНИТЕЛЯ**;

3. изисква от **ИЗПЪЛНИТЕЛЯ** да сключи и да му представи договори за подизпълнение с посочените в офертата му подизпълнители.

Чл. 9. ВЪЗЛОЖИТЕЛЯТ е длъжен да:

1. оказва необходимото съдействие на **ИЗПЪЛНИТЕЛЯ** за изпълнение на задълженията, произтичащи от договора;

2. приеме доставения софтуер при качествено и точно изпълнение на задълженията от страна на **ИЗПЪЛНИТЕЛЯ**;

3. да използва доставения софтуер съобразно предназначението му и предписанията на производителя;

4. да заплати цената при извършване на доставката при качествено и точно изпълнение на задълженията, съгласно клаузите на настоящия договор.

Чл. 10. ИЗПЪЛНИТЕЛЯТ има право:

1. при пълно, точно и навременно изпълнение на задълженията си да получи уговореното възнаграждение при условията и в сроковете, посочени в настоящия договор;

2. да иска от **ВЪЗЛОЖИТЕЛЯ** необходимото съдействие за осъществяване на задълженията си по договора;

3. да иска от **ВЪЗЛОЖИТЕЛЯ** приемане на доставката, когато тя отговаря на изискванията, посочени в настоящия договор и приложенията към него.

Чл. 11. ИЗПЪЛНИТЕЛЯТ е длъжен да:

1. изпълни поръчката, предмет на настоящия договор, в срок и качествено, в съответствие с изискванията на Техническата спецификация и Техническото предложение, които представляват неразделна част от настоящия договор;

2. информира текущо **ВЪЗЛОЖИТЕЛЯ** за хода на изпълнението на настоящия договор и да го уведомява за всяко възникнало събитие, което би довело до забава и/или неизпълнение на задължение по договора и да предложи мерки за неговото преодоляване;

3. да извършва гаранционно обслужване на доставения софтуер съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него,

4. да предоставя всички нови версии на софтуерните продукти, с оказване на необходимото съдействие на **ВЪЗЛОЖИТЕЛЯ** за изтеглянето им и за работата с тях;

5. да предоставя информация по запитвания и заявки от страна на **ВЪЗЛОЖИТЕЛЯ** във връзка с ползването на продуктите;

5.1. да оказва висококвалифицирана специализирана помощ и съдействие за отстраняването на възникнали инциденти и проблеми;

5.2. да отстранява възникнали грешки в софтуера и своевременното да го обновява;

5.3. да осигури свободно и безпрепятствено ползване на продуктите за срока на действие на доставените за тях лицензи *(когато е приложимо).*

6. да уведоми незабавно **ВЪЗЛОЖИТЕЛЯ** при възникване на пречки от стопански, административен или друг характер, които могат да забавят или да направят невъзможно изпълнението на този договор, като може да поиска от **ВЪЗЛОЖИТЕЛЯ** указания и/или съдействие за отстраняването им.

VI. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл. 12. (1) При подписването на този договор, **ИЗПЪЛНИТЕЛЯТ** предоставя на **ВЪЗЛОЖИТЕЛЯ** гаранция за изпълнение в размер на 1% (едно на сто) от стойността по чл. 2, ал. 1. („**Гаранцията за изпълнение**") или **14 587,74 лв.** (четиринадесет хиляди петстотин осемдесет и седем лева и седемдесет и четири стотинки).

(2) Гаранцията за изпълнение е предназначена за обезпечаване на задълженията на **ИЗПЪЛНИТЕЛЯ** по договора, както следва:

1. 50% от сумата по ал. 1 – за изпълнение на дейностите по доставка на софтуер;

2. 50 % от сумата по ал. 1 – за изпълнение на дейностите по гаранционно обслужване.

(3) **ИЗПЪЛНИТЕЛЯТ** избира формата на гаранцията в една от следните форми:

1. парична сума внесена по банковата сметка на Възложителя;

2. банкова гаранция; или

3. застраховка, която обезпечава изпълнението чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ.**

Чл. 13. (1) В случай на изменение на договора, извършено в съответствие с този договор и приложимото право, **ИЗПЪЛНИТЕЛЯТ** се задължава да предприеме необходимите действия за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора, в срок до 3 (три) работни дни от подписването на допълнително споразумение за изменението.

(2) Действията за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора могат да включват, по избор на **ИЗПЪЛНИТЕЛЯ**:

1. внасяне на допълнителна парична сума по банковата сметка на **ВЪЗЛОЖИТЕЛЯ**, при спазване на чл. 14 от договора; и/или;

2. предоставяне на документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, при спазване на изискванията на чл. 15 от договора; и/или

3. предоставяне на документ за изменение на първоначалната застраховка или нова застраховка, при спазване на изискванията на чл. 16 от договора.

Чл. 14. (1) Когато гаранцията се предоставя във вид на парична сума, тя се внася по следната банкова сметка на **ВЪЗЛОЖИТЕЛЯ:**

IBAN: BG43CECB979010C7866100;

BIC: CECBBGSF

Банка: „Централна кооперативна банка“ АД

(2) Всички банкови разходи, свързани с преводите на сумата са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 15. (1) Когато като гаранция за изпълнение се представя банкова гаранция, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на банкова гаранция, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, която трябва да отговаря на следните изисквания:

1. да бъде безусловна и неотменяема банкова гаранция във форма, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, и да съдържа задължение на банката-гарант да извърши плащане при първо

писмено искане от **ВЪЗЛОЖИТЕЛЯ**, деклариращ, че е налице неизпълнение на задължение на **ИЗПЪЛНИТЕЛЯ** или друго основание за задържане на Гаранцията за изпълнение по този договор;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на банковата гаранция се удължава или се издава нова.

(2) Всички банкови разходи свързани с откриването и обслужването на банковата гаранция, по усвояването на средства от страна на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, както и при нейното връщане са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 16. (1) Когато като Гаранция за изпълнение се представя застраховка, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на застрахователна полица, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, в която **ВЪЗЛОЖИТЕЛЯТ** е посочен като трето ползващо се лице (бенефициер), която трябва да отговаря на следните изисквания:

1. да обезпечава изпълнението на този договор чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ** в определения в чл. 12, ал. 1 размер;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на гаранцията се удължава или се издава нова.

3. Застрахователната премията по застраховката следва да е платена на сто процента (не се допуска разсрочено заплащане на застрахователната премия) и не може да бъде използвана за обезпечение на отговорността на изпълнителя по друг договор.

(2) Разходите по сключването на застрахователния договор и поддържането на валидността на застраховката за изисквания срок, както и по всяко изплащане на застрахователно обезщетение в полза на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, са за сметка на **ИЗПЪЛНИТЕЛЯ**

Чл. 17. **(1) ВЪЗЛОЖИТЕЛЯТ** освобождава гаранцията за изпълнение, както следва:

1. Сумата по чл. 12, ал. 2, т. 1 се освобождава в срок до 30 (тридесет) дни след окончателното приемане на доставката, ако липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

2. Сумата по чл. 12, ал. 2, т. 2 се освобождава в срок до 30 (тридесет) дни след изтичане на срока на гаранционното обслужване, в случай, че липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

(2) Освобождаването на Гаранцията за изпълнение се извършва, както следва:

1. когато е във формата на парична сума – чрез превеждане на сумата по банковата сметка на **ИЗПЪЛНИТЕЛЯ**, посочена в чл. 12, ал. 1 от договора;

2. когато е във формата на банкова гаранция – чрез връщане на нейния оригинал на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице;

3. когато е във формата на застраховка – чрез връщане на оригинала на застрахователната полица/застрахователния сертификат на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице.

(3) Гаранцията или съответната част от нея не се освобождава от **ВЪЗЛОЖИТЕЛЯ**, ако в процеса на изпълнение на договора е възникнал спор между Страните относно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** и въпросът е отнесен за решаване пред съд. При решаване на спора в полза на **ВЪЗЛОЖИТЕЛЯ** той може да пристъпи към усвояване на гаранциите.

Чл. 18. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи съответна част и да се удовлетвори от Гаранцията за изпълнение, когато **ИЗПЪЛНИТЕЛЯТ** не изпълни някое от неговите задължения по договора, както и в случаите на лошо, частично и забавено изпълнение на което и да е задължение на **ИЗПЪЛНИТЕЛЯ**, като усвои такава част от Гаранцията за изпълнение, която съответства на уговорената в договора неустойка за съответния случай на неизпълнение.

Чл. 19. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи Гаранцията за изпълнение в пълен размер, в следните случаи:

1. при пълно неизпълнение и разваляне на договора от страна на **ВЪЗЛОЖИТЕЛЯ** на това основание;

2. при прекратяване на дейността на **ИЗПЪЛНИТЕЛЯ** или при обявяването му в несъстоятелност.

Чл. 20. Във всеки случай на задържане на Гаранцията за изпълнение, **ВЪЗЛОЖИТЕЛЯТ** уведомява **ИЗПЪЛНИТЕЛЯ** за задържането и неговото основание. Задържането на Гаранцията за изпълнение изцяло или частично не изчерпва правата на **ВЪЗЛОЖИТЕЛЯ** да търси обезщетение в по-голям размер.

Чл. 21. Когато **ВЪЗЛОЖИТЕЛЯТ** се е удовлетворил от Гаранцията за изпълнение и договорът продължава да е в сила, **ИЗПЪЛНИТЕЛЯТ** се задължава в срок до 5 (пет) дни да допълни Гаранцията за изпълнение, като внесе усвоената от **ВЪЗЛОЖИТЕЛЯ** сума по сметката на **ВЪЗЛОЖИТЕЛЯ** или предостави документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, съответно застраховка, така че във всеки момент от действието на договора размерът на Гаранцията за изпълнение да бъде в съответствие с чл. 12, ал. 1 от договора.

Чл. 22. **ВЪЗЛОЖИТЕЛЯТ** не дължи лихва за времето, през което средствата по Гаранцията за изпълнение са престояли при него законосъобразно.

VII. ГАРАНЦИОННО ОБСЛУЖВАНЕ

Чл. 23. (1) **ИЗПЪЛНИТЕЛЯТ** гарантира за срока, посочен в чл. 4, ал. 3, пълната функционална годност на доставения софтуер съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) В рамките на срока по ал. 1 **ИЗПЪЛНИТЕЛЯТ** отстранява за своя сметка всички повреди и/или несъответствия на софтуера.

Чл. 24. (1) **ИЗПЪЛНИТЕЛЯТ** се задължава да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от **ВЪЗЛОЖИТЕЛЯ**. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които **ИЗПЪЛНИТЕЛЯТ** е отстранил проблемите.

(2) В случай, че **ВЪЗЛОЖИТЕЛЯТ** има забележки по представения отчет по ал. 1, **ВЪЗЛОЖИТЕЛЯТ** може да откаже да го подпише. В този случай **ВЪЗЛОЖИТЕЛЯТ** уведомява писмено **ИЗПЪЛНИТЕЛЯ** и в срок до 10 (десет) работни дни от получаване на уведомлението, страните подписват констативен протокол, в който се отразяват направените забележки и се определя срок за тяхното отстраняване. В случай че **ИЗПЪЛНИТЕЛЯТ** откаже да подпише констативния протокол **ВЪЗЛОЖИТЕЛЯТ** има право сам да състави такъв протокол като съдържанието му е задължително за **ИЗПЪЛНИТЕЛЯ**. Приемането се извършва след отстраняване на забележките в установения срок с подписването на коригиран отчет.

(3) Ако забележките не бъдат отстранени в установения срок, **ВЪЗЛОЖИТЕЛЯТ** може да развали договора с едностранно уведомление, отправено до другата страна, без да дава допълнителен срок за изпълнение.

VIII. НЕУСТОЙКИ

Чл. 25. (1) При забавено изпълнение на задълженията по договора от страна на **ИЗПЪЛНИТЕЛЯ** в нарушение на уговорените в този договор срокове, същият заплаща на **ВЪЗЛОЖИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 % (три на сто) от тази сума.

(2) При забава на **ВЪЗЛОЖИТЕЛЯ** за изпълнение на задълженията му за плащане по договора, същият заплаща на **ИЗПЪЛНИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 % (три на сто) от тази сума.

IX. НЕУСТОЙКИ

Чл. 26. (1) При пълно неизпълнение на договора от страна на **ИЗПЪЛНИТЕЛЯ, ВЪЗЛОЖИТЕЛЯТ** усвоява предоставената гаранция за изпълнение.

(2) При забавено изпълнение на задължения по договора от страна на **ИЗПЪЛНИТЕЛЯ** в нарушение на уговорените в този договор срокове, същият заплаща на **ВЪЗЛОЖИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден.

(3) При забава на **ВЪЗЛОЖИТЕЛЯ** за изпълнение на задълженията му за плащане по договора, същият заплаща на **ИЗПЪЛНИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 на сто (три на сто) от тази сума.

(4) При системно (три и повече пъти) неизпълнение на задълженията за сервизно обслужване в гаранционния срок, **ИЗПЪЛНИТЕЛЯТ** дължи на **ВЪЗЛОЖИТЕЛЯ**, неустойка в размер на 0.5 (нула цяло и пет десети на сто) на сто от сумата по чл. 2, ал. 1.

Чл. 27. ВЪЗЛОЖИТЕЛЯТ може да претендира обезщетение за нанесени вреди и пропуснати ползи по общия ред, независимо от начислените неустойки и независимо от усвояването на гаранцията за изпълнение.

IXa. ПОДИЗПЪЛНИТЕЛИ (когато е приложимо)[1]

Чл. 27а. (1) **ИЗПЪЛНИТЕЛЯТ** е длъжен в срок от три дни от сключването на договор за подизпълнение, както и на допълнително споразумение за замяна на посочен в офертата подизпълнител, да изпрати на **ВЪЗЛОЖИТЕЛЯ** копие на договора/допълнителното споразумение, заедно с доказателства, че са изпълнени условията на чл. 66, ал. 2 или ал. 14 от ЗОП.

(2) **ИЗПЪЛНИТЕЛЯТ** носи пълна отговорност за действията и/или бездействията на подизпълнителите си, като участието им при изпълнението на поръчката, не изменя или намалява задълженията на **ИЗПЪЛНИТЕЛЯ**, съгласно настоящия договор. Видът и делът на участието на подизпълнителя/те следва да бъдат същите, като посочените в офертата на **ИЗПЪЛНИТЕЛЯ.**

(3) При сключването на договор/и с подизпълнител/и, офериран/и в офертата на **ИЗПЪЛНИТЕЛЯ,** последният е длъжен да създаде условия, че:

1. приложимите клаузи на договора са задължителни за изпълнение от подизпълнителя/ите;

2. действията на подизпълнителя/ите няма да доведат пряко или косвено до неизпълнение на договора, за което **ИЗПЪЛНИТЕЛЯТ** да иска освобождаването си от отговорност;

[1] Изискванията и условията, предвидени в този раздел се прилагат в случаите, когато Изпълнителят е предвидил използването на подизпълнители

3. при осъществяване на правата си по настоящия договор, **ВЪЗЛОЖИТЕЛЯТ** ще може без ограничения да извършва проверка на дейността и документацията на подизпълнителя/ите;

4. подизпълнителят няма право да превъзлага една или повече от дейностите, които са включени в предмета на договора за подизпълнение.

(4) **ИЗПЪЛНИТЕЛЯТ** може да извършва замяна на посочените подизпълнители за изпълнение на договора, както и да включва нови подизпълнители в предвидените в ЗОП случаи и при предвидените в ЗОП условия.

(5) Сключването на договор с подизпълнител, който не е обявен в офертата на **ИЗПЪЛНИТЕЛЯ** и не е включен по време на изпълнение на договора по предвидения в ЗОП ред или изпълнението на дейностите по договора от лице, което не е подизпълнител, обявено в офертата на **ИЗПЪЛНИТЕЛЯ**, се счита за неизпълнение на договора и е основание за едностранно прекратяване на договора от страна на Възложителя и за усвояване на пълния размер на гаранцията за изпълнение.

(6) Независимо от използването на подизпълнители, отговорността за изпълнение на настоящия договор е на **ИЗПЪЛНИТЕЛЯ.**

Чл. 27б. (1) Когато частта от поръчката, която се изпълнява от подизпълнител, може да бъде предадена като отделен обект на **ИЗПЪЛНИТЕЛЯ** или на **ВЪЗЛОЖИТЕЛЯ**, **ВЪЗЛОЖИТЕЛЯТ** заплаща възнаграждение за тази част директно на подизпълнителя.

(2) Разплащанията по ал. 1 се осъществяват въз основа на искане, отправено от подизпълнителя до **ВЪЗЛОЖИТЕЛЯ** чрез **ИЗПЪЛНИТЕЛЯ**, който е длъжен да го предостави на **ВЪЗЛОЖИТЕЛЯ** в 15-дневен срок от получаването му.

(3) Към искането по ал. 2 **ИЗПЪЛНИТЕЛЯТ** предоставя становище, от което да е видно дали оспорва плащанията или част от тях като недължими.

(4) **ВЪЗЛОЖИТЕЛЯТ** има право да откаже плащане по ал. 2, когато искането за плащане е оспорено, до момента на отстраняване на причината за отказа.

X. ПРЕКРАТЯВАНЕ И РАЗВАЛЯНЕ НА ДОГОВОРА

Чл. 28. (1) Настоящият договор се прекратява:

1. с изпълнение на всички задължения на страните по договора;

2. при настъпване на обективна невъзможност за изпълнение на договора, включително отмяна на изключителните права на системния интегратор за изпълнение на съответните дейности, посредством промяна в нормативната уредба.

3. при настъпване на друга невиновна невъзможност за изпълнение, непредвидено или непредотвратимо събитие от извънреден характер, възникнало след сключването на договора („непреодолима сила"), продължила повече от 45 дни;

4. при прекратяване на юридическо лице – Страна по договора без правоприемство, по смисъла на законодателството на държавата, в която съответното лице е установено;

5. при условията по чл. 5, ал. 1, т. 3 от Закона за икономическите и финансовите отношения с дружествата, регистрирани в юрисдикции с преференциален данъчен режим, контролираните от тях лица и техните действителни собственици.

(2) Настоящият договор може да бъде прекратен:

1. по взаимно съгласие на Страните, изразено в писмена форма;

2. когато за **ИЗПЪЛНИТЕЛЯ** бъде открито производство по несъстоятелност или ликвидация – по искане на **ВЪЗЛОЖИТЕЛЯ;**

Чл. 29. **ВЪЗЛОЖИТЕЛЯТ** прекратява договора в случаите по чл. 118, ал. 1 от ЗОП, без да дължи обезщетение на **ИЗПЪЛНИТЕЛЯ** за претърпени от прекратяването на Договора вреди, освен ако прекратяването е на основание чл. 118, ал. 1, т. 1 от ЗОП. (В последния случай размерът на обезщетението се определя в протокол или споразумение, подписано от Страните, а при непостигане на съгласие – по реда на клаузата за разрешаване на спорове по този договор.)

Чл. 30. (1) Всяка от страните може да развали договора при виновно неизпълнение на съществено задължение на другата страна по договора, при условията и с последиците съгласно чл. 87 и сл. от Закона за задълженията и договорите, чрез отправяне на писмено предупреждение от изправната страна до неизправната и определяне на подходящ срок за изпълнение. Разваляне на договора не се допуска, когато неизпълнената част от задължението е незначителна с оглед на интереса на изправната страна.

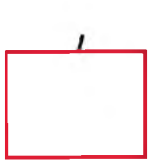
(2) По смисъла на този договор „виновно неизпълнение на съществено задължение на **ИЗПЪЛНИТЕЛЯ**" е:

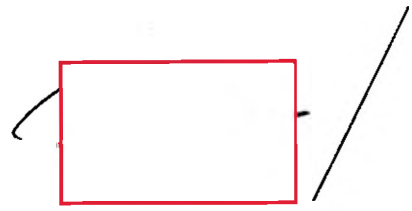
1. когато **ИЗПЪЛНИТЕЛЯТ** забави изпълнението на задължение по настоящия договор с повече от 30 (тридесет) календарни дни;

2. при системно (три или повече пъти) неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционно обслужване и при пълно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционно обслужване;

3. когато **ИЗПЪЛНИТЕЛЯТ** използва подизпълнител, без да е декларирал това в офертата си.

Чл. 31. При предсрочно прекратяване на договора, **ВЪЗЛОЖИТЕЛЯТ** е длъжен да заплати на **ИЗПЪЛНИТЕЛЯ** реално изпълнените и приети по установения ред доставки/услуги.





XI. НЕПРЕОДОЛИМА СИЛА

Чл. 32. (1) Страните се освобождават от отговорност за неизпълнение на задълженията си, когато невъзможността за изпълнение се дължи на непреодолима сила. Никоя от страните не може да се позовава на непреодолима сила, ако е била в забава и не е информирала другата страна за възникването на непреодолима сила.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна незабавно при настъпване на непреодолимата сила.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира.

(4) Не може да се позовава на непреодолима сила онази страна, чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на договора.

XII. КОНФИДЕНЦИАЛНОСТ

Чл. 33. (1) Всяка от страните по този договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата страна, станала известна при или по повод изпълнението на договора („**Конфиденциална информация**“) включително и след прекратяването на същия, неограничено във времето. Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество, или в каквато и да е форма, включително финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни , образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство. Не се смята за конфиденциална информацията, касаеща наименованието на договора, стойността и предмета на този договор, с оглед бъдещо позоваване на придобит професионален опит от **ИЗПЪЛНИТЕЛЯ**.

(2) Конфиденциална информация за целите на настоящия договор включва и :

1. съдържанието на данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор.

2. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на Националната агенция за приходите (НАП) и **ВЪЗЛОЖИТЕЛЯ**, комуникации, мрежи и информационни системи на НАП и на **ВЪЗЛОЖИТЕЛЯ**, изготвени в хода на изпълнението на документи и/или всякакви други резултати от изпълнението, разработена в полза на НАП или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. Информацията е станала или става публично достъпна, без нарушаване на този договор от която и да е от страните;

2. Информацията се изисква по силата на закон, приложим спрямо която и да е от страните; или

3. Предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 страната, която следва да предостави информацията, уведомява незабавно другата страна по договора.

(5) Задълженията на **ИЗПЪЛНИТЕЛЯ** във връзка с изискванията за конфиденциалност включват и:

1. задължение да спазва вътрешните правила за достъп и режим на работа до сградите на НАП и на **ВЪЗЛОЖИТЕЛЯ**, когато е приложимо;

2. да спазва всички процедури и изисквания на НАП за работа в информационната инфраструктура на НАП;

3. да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала му известна при или по повод изпълнението на дейностите, предмет на договора.

4. представляващите **ИЗПЪЛНИТЕЛЯ** и лицата, които имат достъп до системите на НАП е необходимо за предоставят подписани декларации за опазване на информацията по образец, утвърден от НАП при подписване на договора и при необходимост от предоставяне на достъп до системите на НАП.

(6) С изключение на случаите, посочени в ал. 4, конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата страна, като това съгласие не може да бъде отказано безпричинно.

(7) Задълженията по опазване от нерегламентиран достъп до конфиденциална информация се отнасят до **ИЗПЪЛНИТЕЛЯ**, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, в това число подизпълнители, като **ИЗПЪЛНИТЕЛЯТ** отговаря за изпълнението на тези задължения от страна на такива лица.

(8) Всяка от страните се задължава да информира другата при нарушаване на изискванията за опазване на поверителност на информацията по този договор.

(9) Задълженията, свързани с неразкриването на Конфиденциалната информация остават в сила и след прекратяване на договора, на каквото и да е основание.

XIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 34. (1) Освен ако са дефинирани изрично по друг начин в този договор, използваните в него понятия имат значението, дадено им в ЗОП, съответно в легалните дефиниции в Допълнителните разпоредби на ЗОП или, ако няма такива за някои понятия – според значението, което им се придава в основните разпоредби на ЗОП.

(2) При противоречие между различни разпоредби или условия, съдържащи се в договора и Приложенията, се прилагат следните правила:

1. специалните разпоредби имат предимство пред общите разпоредби;

2. разпоредбите на Приложенията имат предимство пред разпоредбите на Договора.

(3) В случаите, когато **ИЗПЪЛНИТЕЛЯТ** е представил Общи условия в офертата си, при възникнало противоречие между тях и клаузите на настоящия договор, с приоритет се прилагат клаузите на договора.

Чл. 35. Настоящият договор може да бъде изменян или допълван от страните при условията на чл. 116 от ЗОП.

Чл. 36. (1) Всички уведомления между Страните във връзка с този Договор се извършват в писмена форма и могат да се предават лично или чрез препоръчано писмо, по куриер, по факс, електронна поща или по телефон, което се потвърждава писмено на следните адреси:

1. За **ВЪЗЛОЖИТЕЛЯ**:

Адрес за кореспонденция: гр. София 1504, ул. „Панайот Волов" № 2

Факс: 02/ 943 66 07

e-mail: office@is-bg.net;

тел. 02/942 03 40

2. За **ИЗПЪЛНИТЕЛЯ**:

Адрес за кореспонденция: гр. София, пк 1510,

район „Подуяне", бул. „Владимир Вазов" № 9

Факс: 02/ 903 01 00

e-mail: vtodorov@ciela.com

тел: 02/ 903 00 90

(2) Страните упълномощават следните представители, които да проследяват и приемат изпълнението на задълженията им по настоящия договор, да осъществяват контрол по цялостното изпълнение на Договора и да подписват предвидените в Договора документи (уведомления, протоколи и др.), както следва:

1. За **ВЪЗЛОЖИТЕЛЯ**:

[redacted] Ръководител, информационни и комуникационни технологии, Отдел „Комуникации", e-mail: [redacted]

2. За **ИЗПЪЛНИТЕЛЯ**

[redacted] – изпълнителен директор, [redacted]

(3) За дата на получаване на уведомлението/заявката се счита:

1. датата на предаването – при лично предаване на уведомлението;

2. датата на пощенското клеймо на обратната разписка – при изпращане по пощата;

3. датата на доставка, отбелязана върху куриерската разписка – при изпращане по куриер;

4. датата, посочена в извлечението от факс устройството– при изпращане по факс;

5. датата на която уведомлението/заявката е постъпила в посочената от ИЗПЪЛНИТЕЛЯ информационна система (e-mail) – при изпращане по електронна поща.

(4) Всяка кореспонденция между Страните ще се счита за валидна, ако е изпратена на посочените по-горе адреси (в т.ч. електронни), чрез посочените по-горе средства за комуникация и на посочените лица по ал. 2. При промяна на посочените адреси, телефони и други данни за контакт, съответната Страна е длъжна да уведоми другата в писмен вид в срок до 3 (три) работни дни от настъпване на промяната. При неизпълнение на това задължение всяко уведомление ще се счита за валидно връчено, ако е изпратено на посочените по-горе адреси, чрез описаните средства за комуникация и на посочените лица за контакт.

(5) При преобразуване без прекратяване, промяна на наименованието, правноорганизационната форма, седалището, адреса на управление, предмета на дейност, срока на съществуване, органите на

[redacted]

[redacted]

управление и представителство на **ИЗПЪЛНИТЕЛЯ**, същият се задължава да уведоми **ВЪЗЛОЖИТЕЛЯ** за промяната в срок до 3 (три) дни от вписването ѝ в съответния регистър.

Чл. 37. Всички спорове по този договор ще се уреждат чрез преговори между страните, а при непостигане на съгласие, ще се отнасят за решаване от компетентния съд в Република България.

Чл. 38. За всички неуредени в този договор въпроси се прилагат разпоредбите на действащото законодателство.

Неразделна част от настоящия договор са:

1. Техническа спецификация на **ВЪЗЛОЖИТЕЛЯ** – Приложение № 1;

1.1. Приложение № 1.8 – Техническа спецификация, относима към обособена позиция № 8 с предмет „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията" - Приложение № 1.8 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*

2. Техническо предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 2.8;

3. Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.8.

При подписване на договора, се представиха следните документи:

1. Гаранция за изпълнение на договора;

2. Документи по чл. 112, ал. 1 от ЗОП.

Настоящият договор се състави в 2 (два) еднообразни оригинални екземпляра на български език – 1 (един) за **ВЪЗЛОЖИТЕЛЯ** и 1 (един) за **ИЗПЪЛНИТЕЛЯ**, и се подписа, както следва:

ЗА ВЪЗЛОЖИТЕЛЯ:

[redacted]

Ивайло Филипов

Изпълнителен директор

[redacted]

.....

Камелия Софрониева

Главен счетоводител

ЗА ИЗПЪЛНИТЕЛЯ:

[redacted]

.....

(подпис и печат)

Веселин Тодо[redacted]

Изпълнителен директор

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ПО ОТКРИТА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ“

I. ПРЕДМЕТ НА ОБЩЕСТВЕНАТА ПОРЪЧКА

1. В предмета на обществената поръчка по обособени позиции №1, № 2, № 3, № 4, № 5, № 6 и № 9 се включват следните дейности:

1.1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването“), подробно описани по вид, количество и технически характеристики в настоящата Техническата спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

1.2. гаранционно обслужване на доставеното по т. 1.1. оборудване, осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

2. В предмета на обществената поръчка по обособени позиции № 7 и № 8 се включват следните дейности:

2.1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер“ или „доставките“), подробно описан по вид, количество и технически характеристики в настоящата Техническа спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

2.2. гаранционно обслужване на доставения софтуер по т. 2.1 (наричано алтернативно „гаранция и поддръжка“), осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ПОРЪЧКАТА

1. Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ".

Важно! *Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

2. Оборудването, предмет на доставката, се състои от хардуер и софтуер, които трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в настоящата Техническа спецификация и/или приложенията към нея. За целта участникът представя към Техническото си предложение по съответната обособена позиция подробно описание на предлаганото от него оборудване/предлагания софтуер.

3. Оборудването (хардуер и софтуер), предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя към датата на сключване на договора за възлагане на обществената поръчка и да не е спряно от производство.

4. Хардуерните компоненти на оборудването трябва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

5. Оборудването следва да бъде доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства да се представят на електронен носител за всеки тип от предлаганите устройства.

6. При доставката на софтуер следва да бъдат предоставени необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера.

III. УСЛОВИЯ НА ДОСТАВКА

1. Доставката на оборудването (хардуер и софтуер) се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка. В писмената заявка се посочват:

1.1. Вид и количество на оборудването (хардуер и софтуер), което следва да бъде доставено;

1.2. Място на доставка на оборудването (хардуер и софтуер);

1.3. Срок на доставка, съобразен със сроковете и условията на доставка по договора за обществена поръчка.

1.4. Друга информация по преценка на възложителя, относима към изпълнението на договора за обществена поръчка.

2. Приемането и предаването на изпълнението се осъществява въз основа на изискванията на договора за обществена поръчка.

IV. ГАРАНЦИЯ И ПОДДРЪЖКА. УСЛОВИЯ НА ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Участникът, избран за изпълнител, гарантира за срока, посочен в т. V.2., пълната функционална годност на доставеното оборудване/доставения софтуер съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него.

2. В рамките на срока по посочен в т. V.2. и в съответствие с режима на гаранционно обслужване участникът, избран за изпълнител, отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

3. Режимът на гаранционното обслужване на хардуера е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч.

4. Времето за реакция на избрания за изпълнител участник е до следващия работен ден от уведомяването му.

** Време за реакция е времето от момента на уведомяване от страна на Възложителя за възникнал проблем до обратна реакция (обаждане или пристигане на място) от участника, избран за изпълнител.*

5. Избраният за изпълнител участник е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.

6. Избраният за изпълнител участник се задължава да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местоположение на оборудването.

7. При невъзможност за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, следва да бъде осигурено оборотно оборудване, притежаващо

характеристиките в Техническото предложение на участника, избран за изпълнител, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

8. В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, избраният за изпълнител участник е длъжен да го замени с ново, с параметри гарантиращи същата или по-добра функционалност и производителност.

9. За всяка извършена дейност, избраният за изпълнител участник изготвя и предоставя протокол, който съдържа описание на извършеното. Протоколът се подписва от представители на двете страни.

10.Избраният за изпълнител участник следва да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от възложителя. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които избраният за изпълнител участник е отстранил проблемите.

11.Всички разходи по време на гаранционното обслужване да са за сметка на избрания за изпълнител участник.

V. СРОК НА ИЗПЪЛНЕНИЕ

1. Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по т. III.1.

2. Срокът на гаранционно обслужване е минимум 5 (пет) години, считано от датата на приемо-предавателния протокол за доставка на оборудването (хардуер и софтуер). Участникът следва да посочи в офертата си срок на гаранционно обслужване, който да отговаря на съответните изисквания.

VI. МЯСТО НА ИЗПЪЛНЕНИЕ

1. Мястото на извършване на доставката е на територията на гр. София, като конкретния адрес на извършване на доставката ще бъде посочен в писмената заявка по т. III.1. .

2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.

VII. ДРУГИ ИЗИСКВАНИЯ. ДОКУМЕНТИ КЪМ ОФЕРТАТА НА УЧАСТНИКА

1. В случай, че не е производител участникът следва да е упълномощен от производителя или от официален представител на производителя за доставка и гаранционно обслужване на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на територията на Република България.

За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлаганото оборудване. Горепосоченият документ се представя в техническото предложение на участника.

Забележка: *В случаите на представяне от участника на оторизационно писмо от официален представител на производителя, в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлаганото оборудване.*

2. Участникът следва да представи Общи условия или други приложими условия за гаранционно обслужване от производителя на продуктите, предмет на обществената поръчка, като ги приложи към техническото си предложение по съответната обособена позиция, в случай, че е приложимо.

VIII. ПРИЛОЖЕНИЯ:

1. Техническа спецификация по обособена позиция № 1 с предмет: **„Доставка на централен процесорен блок за обработка на информация, софтуерни пакети и операционни системи за виртуализация и сървъри за точно време "** – Приложение № 1.1.;

2. Техническа спецификация по обособена позиция № 2 с предмет: **„Доставка на софтуерно дефинирана мрежа за пренос на данни"** – Приложение № 1.2.;

3. Техническа спецификация по обособена позиция № 3 с предмет: **„Доставка на система за филтриране, проследяване и блокиране на Интернет трафик, система за управление на технически уязвимости и защитни стени за граничен слой"** – Приложение № 1.3.;

4. Техническа спецификация по обособена позиция № 4 с предмет: **„Доставка на дискови масиви за данни и хардуерни устройства и софтуерни пакети за създаване на резервни копия и възстановяване на данни"** – Приложение № 1.4.;

5. Техническа спецификация по обособена позиция № 5 с предмет: **„Доставка на софтуерни пакети и хардуерни устройства за дефиниране на опорна мрежа, мрежово оборудване за достъп до масивите за данни, защитни стени за интернет трафик и електронна поща и за локална мрежа"** – Приложение № 1.5.";

6. Техническа спецификация по обособена позиция № 6 с предмет **„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“** – Приложение № 1.6.

7. Техническа спецификация по обособена позиция № 7 с предмет: **„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“** – Приложение № 1.7.;

8. Техническа спецификация по обособена позиция № 8 с предмет: **„Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“** – Приложение № 1.8.;

9. Техническа спецификация по обособена позиция № 9 с предмет: **„Доставка на хардуерни устройства и софтуерни пакети за платформа за управление на събития и сигурността на информацията“** – Приложение № 1.9.

Приложение № 1.8.

Техническа спецификация по обособена позиция № 8 с предмет:
„Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“

1. **Платформа за управление на идентичността на потребителите**

Общи изисквания	
REQ.1.	Тип лиценз: вечен (perpetual), с включени 60 месеца поддръжка
REQ.2.	Брой лицензи: • 1 брой базова система за управление и контрол на цифровите идентичности и достъпа до информация, включени 60 месеца поддръжка на системата; • допълнителни лицензи за модул за 8000 потребителя за функции за контрол на достъпа до информация (access management), включени 60 месеца поддръжка на модула; • допълнителни лицензи за модул за 8000 потребителя за функции за управление и контрол на цифровите идентичности (identity management), включени 60 месеца поддръжка на модула; • допълнителни лицензи за модул за 8000 потребителя за функции за защитено вписване на потребителите в системите (secure login), включени 60 месеца поддръжка на модула;
REQ.3.	Да може да се управлява създаването на акаунти.
REQ.4.	Да може да се управлява промяната на правата, свързани с акаунт.
REQ.5.	Да може да се управлява де-активирането на акаунти (account revocation).
REQ.6.	Да разполага с автоматизирани работни процеси (workflows) за заявяване и одобрение на права за достъп до ресурси.
REQ.7.	Да предоставя възможност, потребителите сами да заявяват и сменят пароли – услуга тип „Password Self-Service”.
REQ.8.	Да предоставя възможност за заявяване и одобрение на услуга за самообслужване.
REQ.9.	Да могат да се наблюдават дейностите на потребителите.
REQ.10.	Да извършва одит на правата за достъп.
REQ.11.	Да предоставя отчети за доказване на съответствие със законови и нормативни документи.
REQ.12.	Да разполага с централизирано хранилище за съхранение на информация за цифрови идентичности, прости роли, композитни роли, упълномощавания, права на достъп.
REQ.13.	Да извършва одит на дейностите, свързани с даване / промяна / отнемане на права и да предосатвя отчети.
REQ.14.	Да могат да се наблюдават централизирано дейностите, свързани с даване / промяна / отнемане на права.
REQ.15.	Да предоставя управление на роли.
REQ.16.	Да предоставя управление на атестации на роли.
REQ.17.	Да предоставя управление на функциите по самообслужването на потребителите (self-service).
REQ.18.	Де е възможно първоначално конфигуриране на решението в среда без мрежова свързаност и след проверка на функционалността – внедряване в реална продукционна среда.

REQ.19.	Да предоставя графично представяне на компонентите на решението за управление на цифрови идентичности (ЦИ) и наблюдение на взаимодействието им и съвместната им работа.
REQ.20.	Да предоставя възможност за модифициране и тестване на средата на решението за управление на ЦИ.
REQ.21.	Да предоставя възможност за пренасяне от тестовата среда в реалната продукционна среда на част от решението или на цялото решение.
REQ.22.	Да предоставя възможност за съвместна работа и споделяне на няколко екипа по внедряване.
REQ.23.	Да извършва анализиране, обогатяване и разширяване на ЦИ. Контролиране на източниците на ЦИ в рамките на организацията.
REQ.24.	Да извършва асоцииране на атрибутите на базата данни с ЦИ на приложенията към базата с данни с ЦИ на решението за управление на ЦИ (schema map attributes association).
REQ.25.	Да извършва анализ на данните за ЦИ, намиране на противоречия, изчистване на данни за ЦИ, осъществяване на съответствие между подобни величини между приложните системи и решението за управление на ЦИ.
REQ.26.	Да позволява дефиниране и конфигуриране на профили за анализиране на един или повече набори от данни.
REQ.27.	Да предоставя метрични данни за сравнение на стойности на атрибути за определяне на съответствието между форматите на данни за ЦИ в приложните системи и в системата за управление на ЦИ.
REQ.28.	Да предоставя профили на съответствието за сравнение на стойности в един или повече набори от данни за ЦИ.
REQ.29.	Да може да открива дублиране на стойности в един набор от данни за ЦИ.
REQ.30.	Да може да открива съответствие между стойности в два различни набора от данни за ЦИ.
REQ.31.	Да предоставя дефиниране на набори от разрешения за достъп, свързани с една или повече приложни системи.
REQ.32.	Да предоставя събиране на идентификатори на акаунти от свързаните системи и свързаните с тях разрешения за достъп.
REQ.33.	Да предоставя централизирано разрешение на достъп на потребителите до свързаните приложни системи.
REQ.34.	Да разполага с вградени роли с различни нива на достъп към модула за управление на роли.
REQ.35.	Да позволява откриване на прости роли, композитни роли, профили.
REQ.36.	Да позволява съпоставяне на прости роли, композитни роли, профили - от различни приложни системи към системата за управление на ЦИ.
REQ.37.	Да предоставя централизирано управление на прости роли, композитни роли и профили, в различните свързани приложни системи.
REQ.38.	Да предоставя автоматизирано средство за изваждане на информация за роли от свързаните системи и връзка с централното хранилище на ЦИ и да разполага с изглед (dashboard) за даване / промяна / отнемане на права.
REQ.39.	Да може да се управлява централизирано чрез уеб-браузър. Централизирано наблюдение, конфигуриране и администриране на системата.

REQ.40.	Да предоставя информация в реално време за здравето на системата и нейните компоненти.
REQ.41.	Да предоставя синхронизиране, трансформиране, разпределяне и обмен на информация за ЦИ в рамките на организацията между свързани системи и системата за управление на ЦИ.
REQ.42.	Да предоставя контрол върху потоците от данни между свързаните системи.
REQ.43.	Да позволява определяне на кои данни да се споделят.
REQ.44.	Да позволява определяне на коя система е авторитарния източник на съответната порция данни.
REQ.45.	Да позволява определяне на това как данните да се интерпретират и трансформират, за да съответстват на изискванията на другите системи.
REQ.46.	Да предоставя синхронизиране на пароли между различни системи.
REQ.47.	Да предоставя автоматизирано създаване на нови потребителски акаунти в свързаните системи.
REQ.48.	Да предоставя автоматизирано премахване на стари потребителски акаунти в свързаните системи.
REQ.49.	Да предоставя отчет за доказване, че точните хора имат разрешен достъп до точните ресурси.
REQ.50.	Да предоставя отчет за доказване, че хората с отнети права нямат права за достъп в системите, за които са им отнети правата на достъп.
REQ.51.	Да предоставя отчет за доказване, че всеки служител има права за достъп до всички ресурси, които се изискват от неговата позиция.
REQ.52.	Да предоставя проследяване на всички дейности свързани с даване / промяна / отнемане на права.
REQ.53.	Да предоставя записване на всички дейности свързани с даване / промяна / отнемане на права.
REQ.54.	Да има възможност за предоставяне на данни за дейностите по даване / промяна / отнемане на права, както и за цифровите идентичности в организацията за целите на вътрешен или външен одит.
REQ.55.	Да предоставя предварително зададени отчети за информация свързана с ЦИ.
REQ.56.	Да предоставя възможност за изработване на специфични отчети, търсения и справки за информация свързана с ЦИ.
REQ.57.	Да предоставя централна мета-директория за съхранение на данни за ЦИ. Метадиректорията да има възможност да е свързана с всички източници на данни за ЦИ и да може да обменя данни за ЦИ със източниците на ЦИ на свързаните системи.
REQ.58.	Да предоставя автоматизиране на обработването и синхронизирането на промените на данните, които настъпват, както в централната мета-директория, така и в отделните системи. Автоматизацията да работи на базата на събития (event-based).
REQ.59.	Да предоставя стандартно вградени драйвери за свързване на външни системи към централната мета-директория и системата за управление на ЦИ.
REQ.60.	Да предоставя възможност за разработване на специфични драйвери за свързване на специфични системи към системата за управление на ЦИ и централната мета-директория.
REQ.61.	Да предоставя възможност за свързване с отдалечени сървъри и системи.

REQ.62.	Да предоставя централизирано хранилище за събиране на всичката информация свързана с ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп.
REQ.63.	Да предоставя възможност за извършване на търсения - както стандартни, така и специфични, дефинирани от потребителя относно: ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп.
REQ.64.	Да предоставя вградени справки за доказване на съответствия с вътрешни / нормативни / законови актове.
REQ.65.	Да предоставя възможност за създаване на специфични отчети.
REQ.66.	Да предоставя автоматизирана услуга за събиране на данните свързани с ЦИ.
REQ.67.	Да предоставя автоматизирана услуга за събиране на данни за свързани системи / акаунти за съответна система / права на достъп / стойности на величини / профили на потребители.
REQ.68.	Да предоставя автоматизирана услуга за регистриране на събития и събиране на одитни записи за дейностите свързани с роли и даване / отнемане / промяна на права, както и за дейности свързани с отчети относно вмъкване, модификация, изтриване или създаване на график за отчет.
REQ.69.	Да предоставя провизиране на потребители, на базата на бизнес-ролята им в организацията.
REQ.70.	Да предоставя автоматизирани работни процеси за одобрение и провизиране.
REQ.71.	Да предоставя атестационен процес на потребители, потребителски профили, роли, задължения.
REQ.72.	Да предоставя откриване и управление на конфликтиращи се роли.
REQ.73.	Да предоставя възможност за самообслужване от страна на потребителите – управление на лични данни, промяна на пароли и секретна лична информация, заявяване на достъп до системи и ресурси.
REQ.74.	Да предоставя надзор над работните процеси за заявяване и одобрение на права.
REQ.75.	Да предоставя уеб-базирана услуга на потребителите за самообслужване.
REQ.76.	Да предоставя автоматизирано провизиране на потребители, на базата на ролята им в организацията.
REQ.77.	Да предоставя персонализиран изглед на потребителите относно разрешения, задачи, заявки.
REQ.78.	Да предоставя самообслужване за нулиране / смяна на пароли.
REQ.79.	Да предоставя възможност за свързване с външни програми за управление на забравени пароли.
REQ.80.	Да предоставя вграден механизъм за единствен доставчик на информация за еднократно вписване (Single Sign-On).
REQ.81.	Да разполага с Common Criteria сертификат от ниво EAL3+.
REQ.82.	Да разполага със сертификати: RHEL 6/7 (за 32 и 64 битови системи).
REQ.83.	Да предоставя защита на уеб-базираните ресурси, като осигурява достъп само на оторизирани потребители до предварително зададени ресурси.
REQ.84.	Да може да осигурява достъп на следните групи потребители: вътрешни служители, външни партньори, външни потребители.

REQ.85.	Да предоставя скриване на адресите на защитените ресурси, както от вътрешни, така и от външни потребители.
REQ.86.	Да може да осигурява достъп до ресурси на оторизирани потребители, без значение, както на местонахождението на потребителя, така и на вида/типа устройство, от което се извършва достъпа.
REQ.87.	Да предоставя управление на множество пароли на един и същ потребител.
REQ.88.	Да може да осигурява достъп само до предварително дефинирани ресурси, в зависимост от позицията/ролята на потребителя в организацията.
REQ.89.	Да предоставя защита на личните данни и да може да осигурява поверителността на потребителите.
REQ.90.	Да разполага с вградени ресурси за изграждане на строга автентификация с повече от един фактор.
REQ.91.	Да предоставя възможност за използване на едни и същи данни за вписване за достъп до услуги от външни доставчици на услуги.
REQ.92.	Да предоставя автоматизирано създаване на потребителски акаунти в системите на федерираните партньори или доставчици на услуги.
REQ.93.	Да предоставя достъп до множество уеб-приложения с еднократна автентикация (с една парола) тип „Single Sign-On", на базата на стандарти.
REQ.94.	Да позволява изграждането и налагането на политики за права за достъп.
REQ.95.	Да предоставя автоматизиране на даването и отнемането на права за достъп, на базата на ролята на потртебителя в организацията и политиките за достъп, свързани с ролята.
REQ.96.	Да предоставя следния модел за автоматизиране на процеса по даването и отнемането на права за достъп:
REQ.97.	Автентикация на потребител -> присъединяване на роля -> преглед на политиките за достъп, свързани с ролята -> налагане на политиките -> осигуряване на достъп до предварително зададени ресурси, в зависимост от ролята.
REQ.98.	Да предоставя възможност за споделяне на информация за цифрова идентичност между различни източници на информация за ЦИ – както вътрешни за организацията, така и външни.
REQ.99.	Да предоставя възможност на външни потребители да получават оторизиран достъп до вътрешни за организацията уеб-ресурси.
REQ.100.	Да поддържа следните стандарти за федериране на ЦИ: Liberty Alliance, WS-Federation, WS-Trust, SAML.
REQ.101.	Да предоставя възможност за идентифициране на риска, свързан с броя на опитите за вписване (login), управление на риска, предприемане на действия, базирани на нивото на риска.
REQ.102.	Да предоставя възможност за определяне на коя бизнес информация или лична информация от корпоративната директория да може да бъде споделяна.
REQ.103.	Да предоставя функция за вмъкване на идентичност (identity injection) чрез извличане на информация от директориина услуга и на тази база – възможност за вмъкване на информация в HTML хедъри, възможност за търсене в стрингове или автентификационни хедъри.

REQ.104.	Да предоставя функция за федериране на идентичност чрез асоцииране на акаунти между доставчик на идентичност и доставчик на услуга.
REQ.105.	Да се поддържат следните протоколи за федериране на идентичност: Liberty, SAML 1.1, SAML 2.0, Oauth.
REQ.106.	Да предоставя следните методи за автентикация на потребителите: • Чрез потребителско име / парола, • RADIUS • Автентикация на базата на токени, • Автентикация чрез X.509 дигитални сертификати, • Kerberos • Риск-базирана автентикация, • Time-Based One-Time Password (TOTP) • „Social authentication“ метод • OpenID Connect
REQ.107.	Да предоставя контрол на правата на потребителите.
REQ.108.	Да предоставя възможност за динамично налагане на политиките за оторизация.
REQ.109.	Да предоставя потребителски портал с възможност за конфигуриране на елементите в него за всеки потребител персонално, където потребителят да може да достъпва и управлява автентификациите си, федерациите и данните на профила си.
REQ.110.	Да предоставя възможност потребителския портал и уеб-страницата за вписване в него да могат да се ребрандират с логото и данните на организацията.
REQ.111.	Да предоставя възможност за интегриране със следните системи за съхраняване на данните за идентификацията и правата на потребителите: • Informix 10 и Informix 12; • IBM Domino 8.5 и IBM Domino 9; • IBM DB2 10; • MS Active Directory реализирана върху MS Windows Server 2008 R2; • MySQL 5.0 -5.5; • CoachDB 10; • LDAP базирани хранилища; • PostgreSQL 8.x и 9.x;
Гаранция и поддръжка:	
REQ.112.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.113.	Получаване на нови версии на софтуера - минимум 5 (пет) години.

2. **Система системата за управление на привилегированите потребители**

Общи изисквания	
REQ.114.	Тип лиценз: вечен (perpetual), с включени 60 месеца поддръжка

REQ.115.	Брой лицензи: софтуерни лицензи за 300 бр. за управление на привилегированите потребители (privileged access management), с включени 60 месеца поддръжка на модула
REQ.116.	Да поддържа управление на правата за достъп до: Windows, Linux, Unix системи; виртуални сървъри; облачни услуги; бази от данни; приложения.
REQ.117.	Да предоставя запис на всички Windows, Linux и Unix команди, извършени от привилегированите потребители на системите.
REQ.118.	Да предоставя видеозапис на сесиите до всички физически и виртуално базирани среди, изискващи удостоверяване на достъпа.
REQ.119.	Да предоставя възможност за търсене във видеозаписите.
REQ.120.	Да предоставя възможност за съхраняване на пароли, ключове и друга чувствителна информация в единно защитено хранилище.
REQ.121.	Да може да извършва корелация на команди, спрямо разрешени такива.
REQ.122.	Да предоставя пълен регистър на възникналите събития, с възможност за одитиране.
REQ.123.	Да може да извършва проверка на пароли за облачни услуги.
REQ.124.	Да поддържа x11 протокол.
REQ.125.	Да предоставя защита на паролите в единно защитено хранилище.
REQ.126.	Да предоставя възможност за допълнителна дву-факторна и стъпкова автентификация.
REQ.127.	Да предоставя поддръжка на допълнителни методи за автентификация чрез – еднократна парола, смартфон, глас, SMS.
REQ.128.	Да поддържа функция за еднократно вписване (Single Sign-On) за Linux и Unix сървъри.
REQ.129.	Да поддържа използването на защитен RDP прокси протокол за отдалечени сесии.
REQ.130.	Да поддържа използването на AD и LDAP автентификация.
REQ.131.	Да предоставя криптирана база от данни за съхранение на данните за вписване на привилегированите потребители.
REQ.132.	Да предоставя възможност за задаване и налагане на политики за управление на достъпа.
REQ.133.	Да предоставя възможност за автоматично идентифициране на привилегированите акаунти.
REQ.134.	Решението да се управлява чрез централизирана уеб-базирана конзола.
REQ.135.	Решението да разполага с интерфейс за управление на политиките за достъп от тип „drag-and-drop“.
REQ.136.	Да предоставя възможност за използване на съществуващи LDAP директории като място за съхранение на данните за вписване на привилегированите потребители.
REQ.137.	Да предоставя възможност за автоматично прилагане на политики за достъп на Windows групи.
REQ.138.	Да предоставя йерархична структура за изграждане на правила за достъп.
REQ.139.	Да предоставя риск-базиран контрол на сесиите на привилегированите потребители и оцветяване на рисковите сесии, с цел непосредствен контрол.
REQ.140.	Да извършва и предоставя анализ на поведението на привилегированите потребители в реално време.
REQ.141.	Да извършва и предоставя анализ на действията с клавиатура от привилегированите потребители.

REQ.142.	Да предоставя възможност за възпроизвеждане на UNIX, Linux and Windows сесиите на привилегированите потребители.
REQ.143.	Да предоставя одит в реално време на всички Windows хостове.
REQ.144.	Да предоставя автоматични отчети на база предварително зададени правила.
REQ.145.	Да предоставя механизми за защита, които да осигуряват невъзможност за промяна, подмяна или унищожаване на събрани одитни видеозаписи и данни.
REQ.146.	Да предоставя възможност за създаване на работни процеси.
REQ.147.	Да предоставя възможност за FTP одит.
REQ.148.	Да предоставя възможност за задаване на ACL ограничения.
Гаранция и поддръжка:	
REQ.149.	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.150.	Получаване на нови версии на софтуера - минимум 5 (пет) години.

ПРИЛОЖЕНИЕ № 2.8

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 8: „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията “***
Наименование на участника:	***СИЕЛА НОРМА АД***
Правно-организационна форма на участника:	***Акционерно дружество***
Седалище по регистрация и адрес на управление:	***гр. София, пк 1510, район Подуяне, бул. „Владимир Вазов“ № 9***
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	***ЕИК 130199580***
Представляващ	***Веселин Тодоров Тодоров***

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното техническо предложение по горецитираната обособена позиция, съдържащо:

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

I.ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛЕНИЕ НА ПОРЪЧКАТА

В качеството си на представляващ участника, декларирам, че сме запознати с условията на поръчката и с подаването на настоящото предложение удостоверявам следното:

1. Предмет на обществената поръчка:

1.1. Декларирам, че представляваният от мен участник ще изпълни поръчката, съобразявайки се с условията по изпълнение, посочени от възложителя в документацията за обществената поръчка.

1.2. Запознати сме, че съгласно чл. 39, ал. 1 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) с подаването на офертата по настоящата обществена поръчка се счита, че се съгласяваме с всички условия на възложителя, в т.ч. с определения срок за валидност на офертата и с проекта на договор, неразделна част от документацията за обществената поръчка.

1.3. Задължаваме се да извършим следните дейности:

1.3.1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричан по-нататък за краткост „софтуера"), подробно описано по вид, количество и технически характеристики в Техническата спецификация, Приложение 1.8. към нея, относимо към настоящата обособена позиция, за която подаваме оферта и настоящето Техническо предложение.

1.3.2. гаранционно обслужване на доставения по т. 1.3.1. софтуер (наричано по-нататък алтернативно „гаранция и поддръжка"), осигурено в рамките на срока по т. 4.2. в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

1.4. Подробно описание на вида, количеството и техническите характеристики на доставения софтуер е описано, както следва:

1.4.1.Платформа за управление на идентичността на потребителите

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.1.	Тип лиценз: вечен (perpetual), с включени 60 месеца поддръжка	Предлаганата платформа за управление на идентичността на потребителите **Micro Focus Identity & Access Management** е с **лицензиране тип вечен лиценз (perpetual), с включени 60 месеца поддръжка**

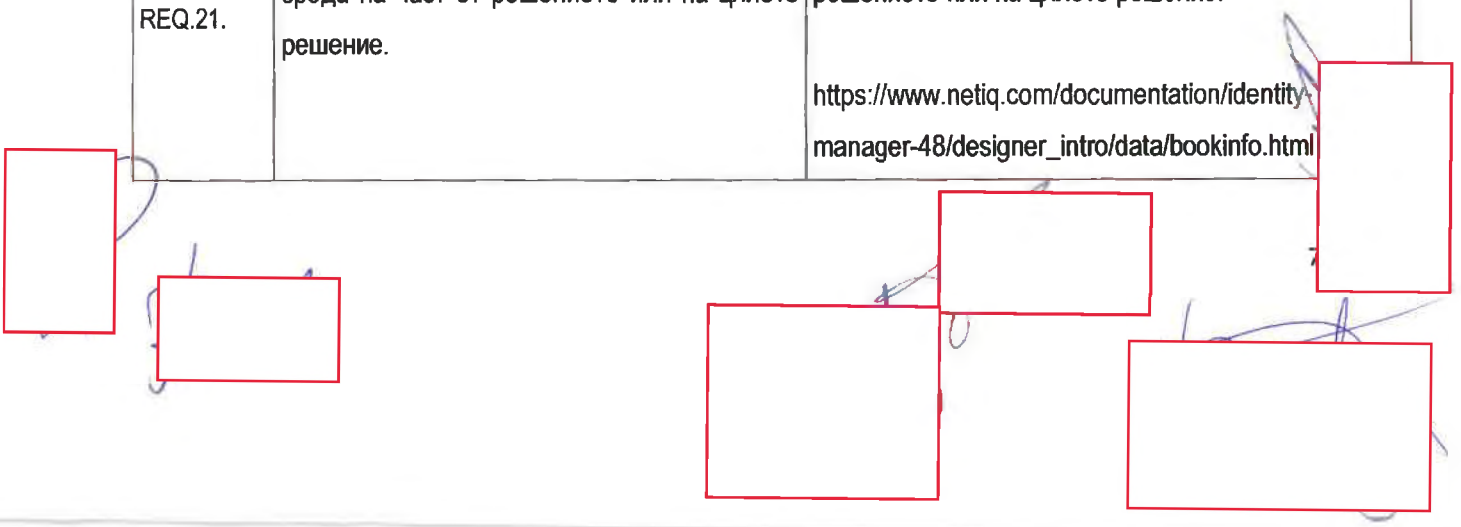
REQ.2.	Брой лицензи: • 1 брой базова система за управление и контрол на цифровите идентичности и достъпа до информация, включени 60 месеца поддръжка на системата; • допълнителни лицензи за модул за 8000 потребителя за функции за контрол на достъпа до информация (access management), включени 60 месеца поддръжка на модула; • допълнителни лицензи за модул за 8000 потребителя за функции за управление и контрол на цифровите идентичности (identity management), включени 60 месеца поддръжка на модула; • допълнителни лицензи за модул за 8000 потребителя за функции за защитено вписване на потребителите в системите (secure login), включени 60 месеца поддръжка на модула;	Предлаганата платформа за управление на идентичността на потребителите включва: • **1 брой базова система за управление и контрол на цифровите идентичности и достъпа до информация Micro Focus Identity & Access Management Base License (per affiliated/enterprise entity) с включена 60-месечна поддръжка;** • **8000 допълнителни лицензи за модул за 8000 потребителя за функции за контрол на достъпа до информация (access management) Micro Focus Access Manager License Add-on (per managed identity) с включена 60-месечна поддръжка към 8000-те лицензa;** • **8000 допълнителни лицензи за модул за 8000 потребителя за функции за управление и контрол на цифровите идентичности (identity management) Micro Focus Identity Management Administration License Add-on (per managed identity) с включена 60-месечна поддръжка към 8000-те лицензa;** • **8000 допълнителни лицензи за модул за 8000 потребителя за функции за защитено вписване на потребителите в системите (secure login) Micro Focus Secure Login License Add-on (per managed identity) с включена 60-месечна поддръжка към 8000-те лицензa;**
REQ.3.	Да може да се управлява създаването на акаунти.	Може да управлява създаването на акаунти. https://www.microfocus.com/media/flyer/identity_

		manager_product_flyer.pdf https://www.microfocus.com/media/data-sheet/access_manager_mds.pdf
REQ.4.	Да може да се управлява промяната на правата, свързани с акаунт.	Може да управлява промяната на правата, свързани с акаунт. https://www.microfocus.com/media/flyer/identity_manager_product_flyer.pdf https://www.microfocus.com/media/data-sheet/access_manager_mds.pdf
REQ.5.	Да може да се управлява де-активирането на акаунти (account revocation).	Може да управлява деактивирането на акаунти (account revocation). https://www.microfocus.com/media/flyer/identity_manager_product_flyer.pdf https://www.microfocus.com/media/data-sheet/access_manager_mds.pdf
REQ.6.	Да разполага с автоматизирани работни процеси (workflows) за заявяване и одобрение на права за достъп до ресурси.	Разполага с автоматизирани работни процеси (workflows) за заявяване и одобрение на права за достъп до ресурси. https://www.netiq.com/documentation/identity-manager-48/form_builder-481/data/form_builder-481.html
REQ.7.	Да предоставя възможност, потребителите сами да заявяват и сменят пароли – услуга тип „Password Self-Service".	Предоставя възможност, потребителите сами да заявяват и сменят пароли – услуга тип „Password Self-Service". https://www.netiq.com/documentation/identity-manager-48/requesting_access/data/

		requesting_access.html
REQ.8.	Да предоставя възможност за заявяване и одобрение на услуга за самообслужване.	Предоставя възможност за заявяване и одобрение на услуга за самообслужване. https://www.netiq.com/documentation/identity-manager-48/requesting_access/data/requesting_access.html
REQ.9.	Да могат да се наблюдават дейностите на потребителите.	Могат да се наблюдават дейностите на потребителите. https://www.netiq.com/documentation/identity-manager-48/security/data/tracking-changes-to-sensitive-information-in-identity-manager.html https://www.netiq.com/documentation/access-manager-45/security-guide/data/b1l1qetc.html
REQ.10.	Да извършва одит на правата за достъп.	Извършва одит на правата за достъп. https://www.netiq.com/documentation/identity-manager-48/security/data/tracking-changes-to-sensitive-information-in-identity-manager.html https://www.netiq.com/documentation/access-manager-45/security-guide/data/b1l1qetc.html https://www.netiq.com/documentation/access-manager-45/admin/data/baizz89.html
REQ.11.	Да предоставя отчети за доказване на съответствие със законови и нормативни документи.	Предоставя отчети за доказване на съответствие със законови и нормативни документи. https://www.netiq.com/documentation/identity-manager-48/security/data/tracking-changes-to-sensitive-information-in-identity-manager.html

		https://www.netiq.com/documentation/access-manager-45/security-guide/data/b1l1qetc.html https://www.netiq.com/documentation/access-manager-45/admin/data/baizz89.html
REQ.12.	Да разполага с централизирано хранилище за съхранение на информация за цифрови идентичности, прости роли, композитни роли, упълномощавания, права на достъп.	Разполага с централизирано хранилище за съхранение на информацията за цифрови идентичности, прости роли, композитни роли, упълномощавания, права на достъп. https://www.netiq.com/documentation/identity-manager-48/setup_windows/data/configuring-identity-vault.html
REQ.13.	Да извършва одит на дейностите, свързани с даване / промяна / отнемане на права и да предосатвя отчети.	Извършва одит на дейностите, свързани с даване / промяна / отнемане на права и може да предоставя отчети. https://www.netiq.com/documentation/access-manager-45/admin/data/baizz89.html
REQ.14.	Да могат да се наблюдават централизирано дейностите, свързани с даване / промяна / отнемане на права.	Могат да се наблюдават централизирано дейностите, свързани с даване / промяна / отнемане на права. https://www.netiq.com/documentation/identity-manager-48/jobs_guide/data/bookinfo.html
REQ.15.	Да предоставя управление на роли.	Предоставя управление на роли. https://www.netiq.com/documentation/identity-manager-48/jobs_guide/data/bookinfo.html
REQ.16.	Да предоставя управление на атестации на роли.	Предоставя управление на атестации на роли. https://www.netiq.com/documentation/identity-

		manager-48/jobs_guide/data/bookinfo.html
REQ.17.	Да предоставя управление на функциите по самообслужването на потребителите (self-service).	Предоставя управление на функциите по самообслужването на потребителите (self-service). https://www.netiq.com/documentation/access-manager-45/admin/data/b1caobu1.html#configuring-sspr
REQ.18.	Да е възможно първоначално конфигуриране на решението в среда без мрежова свързаност и след проверка на функционалността – внедряване в реална продукционна среда.	Има възможност за първоначално конфигуриране на решението в среда без мрежова свързаност и след проверка на функционалността – внедряване в реална продукционна среда. https://www.netiq.com/documentation/identity-manager-48/designer_intro/data/gsdoimsolutions.html
REQ.19.	Да предоставя графично представяне на компонентите на решението за управление на цифрови идентичности (ЦИ) и наблюдение на взаимодействието им и съвместната им работа.	Предоставя графично представяне на компонентите на решението за управление на цифрови идентичности (ЦИ) и наблюдение на взаимодействието им и съвместната им работа. https://www.netiq.com/documentation/identity-manager-48/designer_intro/data/bookinfo.html
REQ.20.	Да предоставя възможност за модифициране и тестване на средата на решението за управление на ЦИ.	Предоставя възможност за модифициране и тестване на средата на решението за управление на ЦИ. https://www.netiq.com/documentation/identity-manager-48/designer_intro/data/bookinfo.html
REQ.21.	Да предоставя възможност за пренасяне от тестовата среда в реалната продукционна среда на част от решението или на цялото решение.	Предоставя възможност за пренасяне от тестовата среда в реалната продукционна среда на част от решението или на цялото решение. https://www.netiq.com/documentation/identity-manager-48/designer_intro/data/bookinfo.html



REQ.22.	Да предоставя възможност за съвместна работа и споделяне на няколко екипа по внедряване.	Предоставя възможност за съвместна работа и споделяне на няколко екипа по внедряване. https://www.netiq.com/documentation/identity-manager-48/designer_intro/data/bookinfo.html
REQ.23.	Да извършва анализиране, обогатяване и разширяване на ЦИ. Контролиране на източниците на ЦИ в рамките на организацията.	Извършва анализиране, обогатяване и разширяване на ЦИ. Има и контролиране на източниците на ЦИ в рамките на организацията. https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_481/data/b2gwxiz.html https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_481/data/b2gx737.html
REQ.24.	Да извършва асоцииране на атрибутите на базата данни с ЦИ на приложенията към базата с данни с ЦИ на решението за управление на ЦИ (schema map attributes association).	Извършва асоцииране на атрибутите на базата данни с ЦИ на приложенията към базата с данни с ЦИ на решението за управление на ЦИ (schema map attributes association). https://www.netiq.com/documentation/identity-manager-48/policy_imanager/data/define-schema-mapping-policies.html
REQ.25.	Да извършва анализ на данните за ЦИ, намиране на противоречия, изчистване на данни за ЦИ, осъществяване на съответствие между подобни величини между приложните системи и решението за управление на ЦИ.	Извършва анализ на данните за ЦИ, намира противоречия, изчиства данните за ЦИ, осъществява съответствие между подобни величини между приложните системи и решението за управление на ЦИ. https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/usinganalyzer.html

REQ.26.	Да позволява дефиниране и конфигуриране на профили за анализиране на един или повече набори от данни.	Позволява дефиниране и конфигуриране на профили за анализиране на един или повече набори от данни. https://www.netiq.com/documentation/identity-manager-48/identity_apps_user_481/data/detailed-identity-manager-dashboard.html
REQ.27.	Да предоставя метрични данни за сравнение на стойности на атрибути за определяне на съответствието между форматите на данни за ЦИ в приложните системи и в системата за управление на ЦИ.	Предоставя метрични данни за сравнение на стойности на атрибути за определяне на съответствието между форматите на данни за ЦИ в приложните системи и в системата за управление на ЦИ. https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/usinganalyzer.html
REQ.28.	Да предоставя профили на съответствието за сравнение на стойности в един или повече набори от данни за ЦИ.	Предоставя профили на съответствието за сравнение на стойности в един или повече набори от данни за ЦИ. https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/usinganalyzer.html
REQ.29.	Да може да открива дублиране на стойности в един набор от данни за ЦИ.	Може да открива дублиране на стойности в един набор от данни за ЦИ. https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/usinganalyzer.html
REQ.30.	Да може да открива съответствие между стойности в два различни набора от данни за ЦИ.	Може да открива съответствие между стойности в два различни набора от данни за ЦИ. https://www.netiq.com/documentation/identity-manager-48/analyzer_admin/data/usinganalyzer.html

REQ.31.	Да предоставя дефиниране на набори от разрешения за достъп, свързани с една или повече приложни системи.	Предоставя дефиниране на набори от разрешения за достъп, свързани с една или повече приложни системи. https://www.netiq.com/documentation/imanager/imanager_admin/data/am757mw.html
REQ.32.	Да предоставя събиране на идентификатори на акаунти от свързаните системи и свързаните с тях разрешения за достъп.	Предоставя събиране на идентификатори на акаунти от свързаните системи и свързаните с тях разрешения за достъп. https://www.netiq.com/documentation/imanager/imanager_admin/data/am757mw.html
REQ.33.	Да предоставя централизирано разрешение на достъп на потребителите до свързаните приложни системи.	Предоставя централизирано разрешение на достъп на потребителите до свързаните приложни системи. https://www.netiq.com/documentation/identity-manager-48/identity_apps_user/data/introduction-to-identity-applications.html
REQ.34.	Да разполага с вградени роли с различни нива на достъп към модула за управление на роли.	Разполага с вградени роли с различни нива на достъп към модула за управление на роли. https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin/data/t44y4268lrdw.html
REQ.35.	Да позволява откриване на прости роли, композитни роли, профили.	Позволява откриване на прости роли, композитни роли, профили. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/netiq-create-manage-roles-identity-manager.html

REQ.36.	Да позволява съпоставяне на прости роли, композитни роли, профили - от различни приложни системи към системата за управление на ЦИ.	Позволява съпоставяне на прости роли, композитни роли, профили - от различни приложни системи към системата за управление на ЦИ. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/netiq-create-manage-roles-identity-manager.html
REQ.37.	Да предоставя централизирано управление на прости роли, композитни роли и профили, в различните свързани приложни системи.	Предоставя централизирано управление на прости роли, композитни роли и профили, в различните свързани приложни системи. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/netiq-create-manage-roles-identity-manager.html
REQ.38.	Да предоставя автоматизирано средство за изваждане на информация за роли от свързаните системи и връзка с централното хранилище на ЦИ и да разполага с изглед (dashboard) за даване / промяна / отнемане на права.	Предоставя автоматизирано средство за изваждане на информация за роли от свързаните системи и връзка с централното хранилище на ЦИ и разполага с изглед (dashboard) за даване / промяна / отнемане на права. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/netiq-create-manage-roles-identity-manager.html
REQ.39.	Да може да се управлява централизирано чрез уеб-браузър. Централизирано наблюдение, конфигуриране и администриране на системата.	Може да се управлява централизирано чрез уеб-браузър. Има централизирано наблюдение, конфигуриране и администриране на системата. https://www.netiq.com/documentation/imanager/imanager_admin/data/am1ox4u.html
REQ.40.	Да предоставя информация в реално време за здравето на системата и нейните компоненти.	Предоставя информация в реално време за здравето на системата и нейните компоненти. https://www.netiq.com/documentation/imanager/

		imanager_admin/data/bz4k320.html
REQ.41.	Да предоставя синхронизиране, трансформиране, разпределяне и обмен на информация за ЦИ в рамките на организацията между свързани системи и системата за управление на ЦИ.	Предоставя синхронизиране, трансформиране, разпределяне и обмен на информация за ЦИ в рамките на организацията между свързани системи и системата за управление на ЦИ. https://www.netiq.com/documentation/identity-manager-48/
REQ.42.	Да предоставя контрол върху потоците от данни между свързаните системи.	Предоставя контрол върху потоците от данни между свързаните системи. https://www.netiq.com/documentation/identity-manager-47/driver_admin/data/b1019sjq.html
REQ.43.	Да позволява определяне на кои данни да се споделят.	Позволява определяне на кои данни да се споделят. https://www.netiq.com/documentation/identity-manager-47/policy_designer/data/smediting.html
REQ.44.	Да позволява определяне на коя система е авторитарния източник на съответната порция данни.	Позволява определяне на коя система е авторитарният източник на съответната порция данни. https://www.netiq.com/documentation/identity-manager-47/policy_understanding/data/netiq-identity-manager-policy-overview.html
REQ.45.	Да позволява определяне на това как данните да се интерпретират и трансформират, за да съответстват на изискванията на другите системи.	Позволява определяне на това, как данните да се интерпретират и трансформират, за да съответстват на изискванията на другите системи. https://www.netiq.com/documentation/identity-manager-48/driver_admin/data/b1019ely.html
REQ.46.	Да предоставя синхронизиране на пароли между различни системи.	Предоставя синхронизиране на пароли между различни системи.

		https://www.netiq.com/documentation/identity-manager-48/
REQ.47.	Да предоставя автоматизирано създаване на нови потребителски акаунти в свързаните системи.	Предоставя автоматизирано създаване на нови потребителски акаунти в свързаните системи. https://www.netiq.com/documentation/identity-manager-48/
REQ.48.	Да предоставя автоматизирано премахване на стари потребителски акаунти в свързаните системи.	Предоставя автоматизирано премахване на стари потребителски акаунти в свързаните системи. https://www.netiq.com/documentation/identity-manager-48/
REQ.49.	Да предоставя отчет за доказване, че точните хора имат разрешен достъп до точните ресурси.	Предоставя отчет за доказване, че точните хора имат разрешен достъп до точните ресурси. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/understanding-the-functionality-of-identity-applications-47.html
REQ.50.	Да предоставя отчет за доказване, че хората с отнети права нямат права за достъп в системите, за които са им отнети правата на достъп.	Предоставя отчет за доказване, че хората с отнети права нямат права за достъп в системите, за които са им отнети правата на достъп. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/understanding-the-functionality-of-identity-applications-47.html
REQ.51.	Да предоставя отчет за доказване, че всеки служител има права за достъп до всички ресурси, които се изискват от неговата позиция.	Предоставя отчет за доказване, че всеки служител има права за достъп до всички ресурси, които се изискват от неговата позиция. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/understanding-the-functionality-of-identity-applications-47.html

REQ.52.	Да предоставя проследяване на всички дейности свързани с даване / промяна / отнемане на права.	Предоставя проследяване на всички дейности свързани с даване / промяна / отнемане на права. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bp2solt.html
REQ.53.	Да предоставя записване на всички дейности свързани с даване / промяна / отнемане на права.	Предоставя записване на всички дейности свързани с даване / промяна / отнемане на права. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bp2solt.html
REQ.54.	Да има възможност за предоставяне на данни за дейностите по даване / промяна / отнемане на права, както и за цифровите идентичности в организацията за целите на вътрешен или външен одит.	Има възможност за предоставяне на данни за дейностите по даване / промяна / отнемане на права, както и за цифровите идентичности в организацията за целите на вътрешен или външен одит. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bp2solt.html
REQ.55.	Да предоставя предварително зададени отчети за информация, свързана с ЦИ.	Предоставя предварително зададени отчети за информация, свързана с ЦИ. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bp2solt.html
REQ.56.	Да предоставя възможност за изработване на специфични отчети, търсения и справки за информация свързана с ЦИ.	Предоставя възможност за изработване на специфични отчети, търсения и справки за информация, свързана с ЦИ. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bp2solt.html
REQ.57.	Да предоставя централна мета-директория за съхранение на данни за ЦИ. Метадиректорията да има възможност да е свързана с всички източници на данни за ЦИ	Предоставя централна мета-директория за съхранение на данни за ЦИ. Метадиректорията има възможност да е свързана с всички източници на

	и да може да обменя данни за ЦИ със източниците на ЦИ на свързаните системи.	данни за ЦИ и може да обменя данни за ЦИ със източниците на ЦИ на свързаните системи. https://www.netiq.com/documentation/identity-manager-47/idm_overview_planning/data/how-identity-manager-works.html
REQ.58.	Да предоставя автоматизиране на обработването и синхронизирането на промените на данните, които настъпват, както в централната мета-директория, така и в отделните системи. Автоматизацията да работи на базата на събития (event-based).	Предоставя автоматизиране на обработването и синхронизирането на промените на данните, които настъпват, както в централната мета-директория, така и в отделните системи. Автоматизацията работи на базата на събития (event-based). https://www.netiq.com/documentation/identity-manager-47/idm_overview_planning/data/how-identity-manager-works.html
REQ.59.	Да предоставя стандартно вградени драйвери за свързване на външни системи към централната мета-директория и системата за управление на ЦИ.	Предоставя стандартно вградени драйвери за свързване на външни системи към централната мета-директория и системата за управление на ЦИ. https://www.netiq.com/documentation/identity-manager-48-drivers/
REQ.60.	Да предоставя възможност за разработване на специфични драйвери за свързване на специфични системи към системата за управление на ЦИ и централната мета-директория.	Предоставя възможност за разработване на специфични драйвери за свързване на специфични системи към системата за управление на ЦИ и централната мета-директория. https://www.netiq.com/documentation/identity-manager-developer/driver-developer-kit.html
REQ.61.	Да предоставя възможност за свързване с отдалечени сървъри и системи.	Предоставя възможност за свързване с отдалечени сървъри и системи. https://www.netiq.com/documentation/identity-manager-47/setup_windows/data/part04e.html

REQ.62.	Да предоставя централизирано хранилище за събиране на всичката информация свързана с ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп.	Предоставя централизирано хранилище за събиране на цялата информация, свързана с ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп. https://www.netiq.com/documentation/identity-manager-47/driver_admin/data/b1019czu.html
REQ.63.	Да предоставя възможност за извършване на търсения - както стандартни, така и специфични, дефинирани от потребителя относно: ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп.	Предоставя възможност за извършване на търсения - както стандартни, така и специфични, дефинирани от потребителя относно: ЦИ, правата за достъп и действията за даване / отнемане / промяна на права за достъп. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bookinfo.html https://www.netiq.com/documentation/sentinel-81/pdfdoc/user/user.pdf
REQ.64.	Да предоставя вградени справки за доказване на съответствия с вътрешни / нормативни / законови актове.	Предоставя вградени справки за доказване на съответствия с вътрешни / нормативни / законови актове. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bookinfo.html
REQ.65.	Да предоставя възможност за създаване на специфични отчети.	Предоставя възможност за създаване на специфични отчети. https://www.netiq.com/documentation/identity-manager-48/report_setup/data/bookinfo.html
REQ.66.	Да предоставя автоматизирана услуга за събиране на данните свързани с ЦИ.	Предоставя автоматизирана услуга за събиране на данните, свързани с ЦИ.

		https://www.netiq.com/documentation/identity-manager-47/report_setup/data/t44br6dr4sch.html
REQ.67.	Да предоставя автоматизирана услуга за събиране на данни за свързани системи / акаунти за съответна система / права на достъп / стойности на величини / профили на потребители.	Предоставя автоматизирана услуга за събиране на данни за свързани системи / акаунти за съответна система / права на достъп / стойности на величини / профили на потребители. https://www.netiq.com/documentation/identity-manager-47/report_setup/data/t44br6dr4sch.html
REQ.68.	Да предоставя автоматизирана услуга за регистриране на събития и събиране на одитни записи за дейностите свързани с роли и даване / отнемане / промяна на права, както и за дейности свързани с отчети относно вмъкване, модификация, изтриване или създаване на график за отчет.	Предоставя автоматизирана услуга за регистриране на събития и събиране на одитни записи за дейностите свързани с роли и даване / отнемане / промяна на права, както и за дейности, свързани с отчети относно вмъкване, модификация, изтриване или създаване на график за отчет. https://www.netiq.com/documentation/identity-manager-47/idm_overview_planning/data/identity-manager-auditing-reporting-guidelines.html
REQ.69.	Да предоставя провизиране на потребители, на базата на бизнес-ролята им в организацията.	Предоставя провизиране на потребители, на базата на бизнес-ролята им в организацията. https://www.netiq.com/documentation/identity-manager-48/
REQ.70.	Да предоставя автоматизирани работни процеси за одобрение и провизиране.	Предоставя автоматизирани работни процеси за одобрение и провизиране. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin_471/data/identity-manager-workflows-47.html

REQ.71.	Да предоставя атестационен процес на потребители, потребителски профили, роли, задължения.	Предоставя атестационен процес на потребители, потребителски профили, роли, задължения. https://www.netiq.com/documentation/identity-manager-48/
REQ.72.	Да предоставя откриване и управление на конфликтиращи се роли.	Предоставя откриване и управление на конфликтиращи се роли. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/netiq-identity-manager-sod-seperation-of-duties.html
REQ.73.	Да предоставя възможност за самообслужване от страна на потребителите – управление на лични данни, промяна на пароли и секретна лична информация, заявяване на достъп до системи и ресурси.	Предоставя възможност за самообслужване от страна на потребителите – управление на лични данни, промяна на пароли и секретна лична информация, заявяване на достъп до системи и ресурси. https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_481/data/using-self-service-password-management-in-identity-manager.html
REQ.74.	Да предоставя надзор над работните процеси за заявяване и одобрение на права.	Предоставя надзор над работните процеси за заявяване и одобрение на права. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin_471/data/identity-manager-workflows-47.html
REQ.75.	Да предоставя уеб-базирана услуга на потребителите за самообслужване.	Предоставя уеб-базирана услуга на потребителите за самообслужване. https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin/data/t44y4268lrdw.html

REQ.76.	Да предоставя автоматизирано провизиране на потребители, на базата на ролята им в организацията.	Предоставя автоматизирано провизиране на потребители, на базата на ролята им в организацията. https://www.netiq.com/documentation/identity-manager-48/
REQ.77.	Да предоставя персонализиран изглед на потребителите относно разрешения, задачи, заявки.	Ппредоставя персонализиран изглед на потребителите относно разрешения, задачи, заявки. https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin/data/t44y4268lrdw.html
REQ.78.	Да предоставя самообслужване за нулиране / смяна на пароли.	Предоставя самообслужване за нулиране / смяна на пароли. https://www.netiq.com/documentation/identity-manager-47/setup_windows/data/windows-self-service-password-management-identity-manager.html
REQ.79.	Да предоставя възможност за свързване с външни програми за управление на забравени пароли.	Предоставя възможност за свързване с външни програми за управление на забравени пароли. https://www.netiq.com/documentation/self-service-password-reset-43/sspr-adminguide/data/t43milg959i5.html
REQ.80.	Да предоставя вграден механизъм за единствен доставчик на информация за еднократно вписване (Single Sign-On).	Предоставя вграден механизъм за единствен доставчик на информация за еднократно вписване (Single Sign-On). https://www.netiq.com/documentation/identity-manager-48/identity_apps_admin_481/data/configure-single-sign-on-access.html

REQ.81.	Да разполага с Common Criteria сертификат от ниво EAL3+.	Разполага с Common Criteria сертификат от ниво EAL3+. https://www.cse-cst.gc.ca/en/publication/netiqr-identity-managertm-45 https://www.prnewswire.com/news-releases/netiq-access-manager-40-earns-eal-3-common-criteria-certification-300021941.html https://www.microfocus.com/media/flyer/identity_manager_the_foundation_for_identity_powered_solutions_flyer.pdf
REQ.82.	Да разполага със сертификати: RHEL 6/7 (за 32 и 64 битови системи).	Разполага със сертификати: RHEL 6/7 (за 32 и 64 битови системи). https://www.netiq.com/documentation/identity-manager48/pdfdoc/releasenotes_idm481/releasenotes_idm481.pdf
REQ.83.	Да предоставя защита на уеб-базираните ресурси, като осигурява достъп само на оторизирани потребители до предварително зададени ресурси.	Предоставя защита на уеб-базираните ресурси, като осигурява достъп само на оторизирани потребители до предварително зададени ресурси. https://www.netiq.com/documentation/access-manager-45/
REQ.84.	Да може да осигурява достъп на следните групи потребители: вътрешни служители, външни партньори, външни потребители.	Може да осигурява достъп на следните групи потребители: вътрешни служители, външни партньори, външни потребители. https://www.netiq.com/documentation/access-manager-45/

REQ.85.	Да предоставя скриване на адресите на защитените ресурси, както от вътрешни, така и от външни потребители.	Предоставя скриване на адресите на защитените ресурси, както от вътрешни, така и от външни потребители. https://www.netiq.com/documentation/access-manager-45/
REQ.86.	Да може да осигурява достъп до ресурси на оторизирани потребители, без значение, както на местонахождението на потребителя, така и на вида/типа устройство, от което се извършва достъпа.	Може да осигурява достъп до ресурси на оторизирани потребители, без значение, както на местонахождението на потребителя, така и на вида/типа устройство, от което се извършва достъпа. https://www.netiq.com/documentation/access-manager-45/
REQ.87.	Да предоставя управление на множество пароли на един и същ потребител.	Предоставя управление на множество пароли на един и същ потребител. https://www.netiq.com/documentation/access-manager-45/admin/data/b1caobtw.html
REQ.88.	Да може да осигурява достъп само до предварително дефинирани ресурси, в зависимост от позицията/ролята на потребителя в организацията.	Може да осигурява достъп само до предварително дефинирани ресурси, в зависимост от позицията/ролята на потребителя в организацията. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/netiq-create-manage-roles-identity-manager.html
REQ.89.	Да предоставя защита на личните данни и да може да осигурява поверителността на потребителите.	Предоставя защита на личните данни и може да осигурява поверителността на потребителите. https://www.netiq.com/documentation/access-manager-45/security-guide/data/bookinfo.html

REQ.90.	Да разполага с вградени ресурси за изграждане на строга автентификация с повече от един фактор.	Разполага с вградени ресурси за изграждане на строга автентификация с повече от един фактор. https://www.netiq.com/documentation/access-manager-45-appliance/security-guide/data/b1l1qk5e.html
REQ.91.	Да предоставя възможност за използване на едни и същи данни за вписване за достъп до услуги от външни доставчици на услуги.	Предоставя възможност за използване на едни и същи данни за вписване за достъп до услуги от външни доставчици на услуги. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b65ogn0.html
REQ.92.	Да предоставя автоматизирано създаване на потребителски акаунти в системите на федерираните партньори или доставчици на услуги.	Предоставя автоматизирано създаване на потребителски акаунти в системите на федерираните партньори или доставчици на услуги. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b65ogn0.html
REQ.93.	Да предоставя достъп до множество уеб-приложения с еднократна автентикация (с една парола) тип „Single Sign-On", на базата на стандарти.	Предоставя достъп до множество уеб-приложения с еднократна автентикация (с една парола) тип „Single Sign-On", на базата на стандарти. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/access-manager-for-single-sign-on.html
REQ.94.	Да позволява изграждането и налагането на политики за права за достъп.	Позволява изграждането и налагането на политики за права за достъп. https://www.netiq.com/documentation/access-manager-45/admin/data/b1dmtq0n.html
REQ.95.	Да предоставя автоматизиране на даването и отнемането на права за достъп, на базата	Предоставя автоматизиране на даването и отнемането на права за достъп, на базата на

	на ролята на потребителя в организацията и политиките за достъп, свързани с ролята.	ролята на потребителя в организацията и политиките за достъп, свързани с ролята. https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/agpropartprovisioning.html
REQ.96.	Да предоставя следния модел за автоматизиране на процеса по даването и отнемането на права за достъп:	Предоставя следния модел за автоматизиране на процеса по даването и отнемането на права за достъп: https://www.netiq.com/documentation/identity-manager-47/identity_apps_admin/data/agpropartprovisioning.html
REQ.97.	Автентикация на потребител -> присъединяване на роля -> преглед на политиките за достъп, свързани с ролята -> налагане на политиките -> осигуряване на достъп до предварително зададени ресурси, в зависимост от ролята.	Процесът е: Автентикация на потребител -> присъединяване на роля -> преглед на политиките за достъп, свързани с ролята -> налагане на политиките -> осигуряване на достъп до предварително зададени ресурси, в зависимост от ролята. https://www.netiq.com/documentation/access-manager-45/
REQ.98.	Да предоставя възможност за споделяне на информация за цифрова идентичност между различни източници на информация за ЦИ – както вътрешни за организацията, така и външни.	Предоставя възможност за споделяне на информация за цифрова идентичност между различни източници на информация за ЦИ – както вътрешни за организацията, така и външни. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b65ogn0.html
REQ.99.	Да предоставя възможност на външни потребители да получават оторизиран достъп до вътрешни за организацията уеб-ресурси.	Предоставя възможност на външни потребители да получават оторизиран достъп до вътрешни за организацията уеб-ресурси.

		https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b65ogn0.html
REQ.100.	Да поддържа следните стандарти за федериране на ЦИ: Liberty Alliance, WS-Federation, WS-Trust, SAML.	Поддържа следните стандарти за федериране на ЦИ: Liberty Alliance, WS-Federation, WS-Trust, SAML. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b65ogn0.html
REQ.101.	Да предоставя възможност за идентифициране на риска, свързан с броя на опитите за вписване (login), управление на риска, предприемане на действия, базирани на нивото на риска.	Предоставя възможност за идентифициране на риска, свързан с броя на опитите за вписване (login), управление на риска, предприемане на действия, базирани на нивото на риска. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b8n3v8l.html
REQ.102.	Да предоставя възможност за определяне на коя бизнес информация или лична информация от корпоративната директория да може да бъде споделяна.	Предоставя възможност за определяне на коя бизнес информация или лична информация от корпоративната директория да може да бъде споделяна. https://www.netiq.com/documentation/netiqaccessmanager4/identityserverhelp/data/b5xz2h6.html
REQ.103.	Да предоставя функция за вмъкване на идентичност (identity injection) чрез извличане на информация от директории на услуга и на тази база – възможност за вмъкване на информация в HTML хедъри, възможност за търсене в стрингове или автентификационни хедъри.	Предоставя функция за вмъкване на идентичност (identity injection) чрез извличане на информация от директории на услуга и на тази база – възможност за вмъкване на информация в HTML хедъри, възможност за търсене в стрингове или автентификационни хедъри. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b5547ku.html

REQ.104.	Да предоставя функция за федериране на идентичност чрез асоцииране на акаунти между доставчик на идентичност и доставчик на услуга.	Предоставя функция за федериране на идентичност чрез асоцииране на акаунти между доставчик на идентичност и доставчик на услуга. https://www.netiq.com/documentation/access-manager-45/admin/data/b1caobu1.html https://www.netiq.com/documentation/access-manager-45/admin/data/b1caoduo.html
REQ.105.	Да се поддържат следните протоколи за федериране на идентичност: Liberty, SAML 1.1, SAML 2.0, Oauth.	Поддържат се следните протоколи за федериране на идентичност: Liberty, SAML 1.1, SAML 2.0, Oauth. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/b65ogn0.htm https://www.netiq.com/documentation/access-manager-45-developer-documentation/oauth-application-developer-guide/data/authorization-endpoint-details.html
REQ.106.	Да предоставя следните методи за автентикация на потребителите: • Чрез потребителско име / парола, • RADIUS • Автентикация на базата на токени, • Автентикация чрез X.509 дигитални сертификати, • Kerberos • Риск-базирана автентикация, • Time-Based One-Time Password (TOTP) • „Social authentication“ метод • OpenID Connect	Предоставя следните методи за автентикация на потребителите: • Чрез потребителско име / парола, • RADIUS • Автентикация на базата на токени, • Автентикация чрез X.509 дигитални сертификати, • Kerberos • Риск-базирана автентикация, • Time-Based One-Time Password (TOTP) • „Social authentication“ метод • OpenID Connect

		https://www.netiq.com/documentation/advanced-authentication-62/server-administrator-guide/data/configuring_method.html#t45gug0lime6
REQ.107.	Да предоставя контрол на правата на потребителите.	Предоставя контрол на правата на потребителите. https://www.netiq.com/documentation/access-manager-45/
REQ.108.	Да предоставя възможност за динамично налагане на политиките за оторизация.	Предоставя възможност за динамично налагане на политиките за оторизация. https://www.netiq.com/documentation/access-manager-45/
REQ.109.	Да предоставя потребителски портал с възможност за конфигуриране на елементите в него за всеки потребител персонално, където потребителят да може да достъпва и управлява автентификациите си, федерациите и данните на профила си.	Предоставя потребителски портал с възможност за конфигуриране на елементите в него за всеки потребител персонално, където потребителят може да достъпва и управлява автентификациите си, федерациите и данните на профила си. https://www.netiq.com/documentation/access-manager-45/admin/data/b1hnzkdu.html
REQ.110.	Да предоставя възможност потребителския портал и уеб-страницата за вписване в него да могат да се ребрандират с логото и данните на организацията.	Предоставя възможност потребителския портал и уеб-страницата за вписване в него да могат да се ребрандират с логото и данните на организацията. https://www.netiq.com/documentation/access-manager-45-appliance/admin/data/branding.html
REQ.111.	Да предоставя възможност за интегриране със следните системи за съхраняване на данните за идентификацията и правата на потребителите: • Informix 10 и Informix 12; • IBM Domino 8.5 и IBM Domino 9; • IBM DB2 10;	Предоставя възможност за интегриране със следните системи за съхраняване на данните за идентификацията и правата на потребителите: • Informix 10 и Informix 12; • IBM Domino 8.5 и IBM Domino 9; • IBM DB2 10;

	• MS Active Directory реализирана върху MS Windows Server 2008 R2; • MySQL 5.0 -5.5; • CoachDB 10; • LDAP базирани хранилища; • PostgreSQL 8.x и 9.x;	• MS Active Directory реализирана върху MS Windows Server 2008 R2; • MySQL 5.0 -5.5; • CoachDB 10; • LDAP базирани хранилища; • PostgreSQL 8.x и 9.x; https://www.netiq.com/documentation/identity-manager-48/system-requirements-identity-manager-48x/data/system-requirements-identity-manager-48x.html#databases https://www.netiq.com/documentation/identity-manager-48-drivers/
Гаранция и поддръжка:		
REQ.112.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническа поддържка е 5 (пет) години.
REQ.113.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Нови версии на софтуера ще се получават 5 (пет) години.

1.4.2. Система системата за управление на привилегированите потребители

Изискано от Възложителя		**Предложено от участника**
А.		**Б.**
Общи изисквания		
REQ.114.	Тип лиценз: вечен (perpetual), с включени 60 месеца поддръжка	Предлаганата системата за управление на привилегированите потребители **Micro Focus Privileged Account Manager** е с **лицензиране тип вечен лиценз (perpetual), с включени 60 месеца поддръжка.**
REQ.115.	Брой лицензи: софтуерни лицензи за 300 бр. за управление на привилегированите	Предлаганата системата за управление на привилегированите потребители включва:

	потребители (privileged access management), с включени 60 месеца поддръжка на модула	**300 софтуерни лицензи за управление на привилегированите потребители (privileged access management) Micro Focus Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices (per managed endpoint) с включена 60-месечна поддръжка към 300-те лицензa;**
REQ.116.	Да поддържа управление на правата за достъп до: Windows, Linux, Unix системи; виртуални сървъри; облачни услуги; бази от данни; приложения.	Поддържа управление на правата за достъп до: Windows, Linux, Unix системи; виртуални сървъри; облачни услуги; бази от данни; приложения. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/t48frmjz9jts.html https://www.netiq.com/documentation/privileged-account-manager-37/npam_install/data/bjh5704.html https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/pam_linux.html
REQ.117.	Да предоставя запис на всички Windows, Linux и Unix команди, извършени от привилегированите потребители на системите.	Предоставя запис на всички Windows, Linux и Unix команди, извършени от привилегированите потребители на системите. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/bjh0h88.html
REQ.118.	Да предоставя видеозапис на сесиите до всички физически и виртуално базирани среди, изискващи удостоверяване на достъпа.	Предоставя видеозапис на сесиите до всички физически и виртуално базирани среди, изискващи удостоверяване на достъпа. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/bjh0h88.html

REQ.119.	Да предоставя възможност за търсене във видеозаписите.	Предоставя възможност за търсене във видеозаписите. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/bjh0h88.html#replay_keystrokes
REQ.120.	Да предоставя възможност за съхраняване на пароли, ключове и друга чувствителна информация в единно защитено хранилище.	Предоставя възможност за съхраняване на пароли, ключове и друга чувствителна информация в единно защитено хранилище. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/b1lf5qip.html https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/command_control_overview.html
REQ.121.	Да може да извършва корелация на команди, спрямо разрешени такива.	Може да извършва корелация на команди, спрямо разрешени такива. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/command_control_overview.html
REQ.122.	Да предоставя пълен регистър на възникналите събития, с възможност за одитиране.	Предоставя пълен регистър на възникналите събития, с възможност за одитиране. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/bjglbku.html
REQ.123.	Да може да извършва проверка на пароли за облачни услуги.	Може да извършва проверка на пароли за облачни услуги. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/t46pvfk3dzz3.html#t46p8ctice3q

REQ.124.	Да поддържа x11 протокол.	Поддържа x11 протокол. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/bjfzqbk.html
REQ.125.	Да предоставя защита на паролите в единно защитено хранилище.	Предоставя защита на паролите в единно защитено хранилище. https://www.netiq.com/documentation/privileged-account-manager-37/pdfdoc/npam_install/npam_install.pdf
REQ.126.	Да предоставя възможност за допълнителна дву-факторна и стъпкова автентификация.	Предоставя възможност за допълнителна дву-факторна и стъпкова автентификация. https://www.netiq.com/documentation/securelogin-88/installation_guide/data/b1k6mouc.html https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/t4ayo9ecmnrx.html
REQ.127.	Да предоставя поддръжка на допълнителни методи за автентификация чрез – еднократна парола, смартфон, глас, SMS.	Предоставя поддръжка на допълнителни методи за автентификация чрез – еднократна парола, смартфон, глас, SMS. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/b1l5epwa.html https://www.netiq.com/documentation/securelogin-88/installation_guide/data/b1k6mouc.html
REQ.128.	Да поддържа функция за еднократно вписване (Single Sign-On) за Linux и Unix сървъри.	Поддържа функция за еднократно вписване (Single Sign-On) за Linux и Unix сървъри.

		https://www.netiq.com/documentation/privileged-account-manager-37/npam_install/data/t46kxgzdq2lh.html
REQ.129.	Да поддържа използването на защитен RDP прокси протокол за отдалечени сесии.	Поддържа използването на защитен RDP прокси протокол за отдалечени сесии. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/b1g0kwp5.html
REQ.130.	Да поддържа използването на AD и LDAP автентификация.	Поддържа използването на AD и LDAP автентификация. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/framework_roles_ldap.html
REQ.131.	Да предоставя криптирана база от данни за съхранение на данните за вписване на привилегированите потребители.	Предоставя криптирана база от данни за съхранение на данните за вписване на привилегированите потребители. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/passwordcheckout.html
REQ.132.	Да предоставя възможност за задаване и налагане на политики за управление на достъпа.	Предоставя възможност за задаване и налагане на политики за управление на достъпа. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/templates.html
REQ.133.	Да предоставя възможност за автоматично идентифициране на привилегированите акаунти.	Предоставя възможност за автоматично идентифициране на привилегированите акаунти. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/

		t45tqvi1mtx6.html
REQ.134.	Решението да се управлява чрез централизирана уеб-базирана конзола.	Решението се управлява чрез централизирана уеб-базирана конзола. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/t41w8v1oxrl6.html
REQ.135.	Решението да разполага с интерфейс за управление на политиките за достъп от тип „drag-and-drop“.	Решението разполага с интерфейс за управление на политиките за достъп от тип „drag-and-drop“. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/user_account_settings.html
REQ.136.	Да предоставя възможност за използване на съществуващи LDAP директории като място за съхранение на данните за вписване на привилегированите потребители.	Предоставя възможност за използване на съществуващи LDAP директории като място за съхранение на данните за вписване на привилегированите потребители. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/brxvkf6.html
REQ.137.	Да предоставя възможност за автоматично прилагане на политики за достъп на Windows групи.	Предоставя възможност за автоматично прилагане на политики за достъп на Windows групи. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/t48frmjz9jts.html#
REQ.138.	Да предоставя йерархична структура за изграждане на правила за достъп.	Предоставя йерархична структура за изграждане на правила за достъп. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/managing_users.html

REQ.139.	Да предоставя риск-базиран контрол на сесиите на привилегированите потребители и оцветяване на рисковите сесии, с цел непосредствен контрол.	Предоставя риск-базиран контрол на сесиите на привилегированите потребители и оцветяване на рисковите сесии, с цел непосредствен контрол. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/compliance_auditor_event_list.html
REQ.140.	Да извършва и предоставя анализ на поведението на привилегированите потребители в реално време.	Извършва и предоставя анализ на поведението на привилегированите потребители в реално време. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/b1kbjw2i.html
REQ.141.	Да извършва и предоставя анализ на действията с клавиатура от привилегированите потребители.	Извършва и предоставя анализ на действията с клавиатура от привилегированите потребители. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/compliance_auditor_event_list.html
REQ.142.	Да предоставя възможност за възпроизвеждане на UNIX, Linux and Windows сесиите на привилегированите потребители.	Предоставя възможност за възпроизвеждане на UNIX, Linux and Windows сесиите на привилегированите потребители. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/compliance_auditor_event_list.html
REQ.143.	Да предоставя одит в реално време на всички Windows хостове.	Предоставя одит в реално време на всички Windows хостове. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/bjglbku.html
REQ.144.	Да предоставя автоматични отчети на база предварително зададени правила.	Предоставя автоматични отчети на база предварително зададени правила.

		https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/command_control_reports.html
REQ.145.	Да предоставя механизми за защита, които да осигуряват невъзможност за промяна, подмяна или унищожаване на събрани одитни видеозаписи и данни.	Предоставя механизми за защита, които осигуряват невъзможност за промяна, подмяна или унищожаване на събрани одитни видеозаписи и данни. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/command_control_reports.html
REQ.146.	Да предоставя възможност за създаване на работни процеси.	Предоставя възможност за създаване на работни процеси. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/t41wusurtnvg.html https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/workflow.html
REQ.147.	Да предоставя възможност за FTP одит.	Предоставя възможност за FTP одит. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/command_control_reports.html
REQ.148.	Да предоставя възможност за задаване на ACL ограничения.	Предоставя възможност за задаване на ACL ограничения. https://www.netiq.com/documentation/privileged-account-manager-37/npam_admin/data/compliance_auditor_acls.html
Гаранция и поддръжка:		

REQ.149.	Срок на техническа поддържка – минимум 5 (пет) години.	Срокът на техническата поддържка е 5 (пет) години.
REQ.150.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Новите версии на софтуера ще се получват 5 (пет) години.

Забележка: а) *Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ". Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

б) *Предметът на доставката трябва да съответства или да надвишава в техническо отношение посочените минимални изисквания в Техническата спецификация и приложението към нея, относимо към настоящата обособена позиция.*

2. Условия на доставка

2.1. Запознати сме, че доставката на софтуера ще се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка.

2.2. Приемането и предаването на изпълнението ще се осъществява въз основа на изискванията на договора за обществена поръчка.

3. Условия на гаранционно обслужване

3.1. Гарантираме за срока, посочен в т. 4.2., пълната функционална годност на доставнения от нас софтуер съгласно предписанията на производителя, изискванията на договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение и приложенията към него.

4. Срок на изпълнение

4.1. Задължаваме се да извършим доставка на софтуера в срок до 10 календарни дни, считано от датата на получаване на писмена заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.

***Забележка**: Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.*

4.2. Срокът на гаранционно обслужване е 5 (пет) години, считано от датата на приемо-предавателния протокол за доставка на софтуера.

***Забележка**: Участникът следва да предложи в офертата си срок за гаранционно обслужване, който следва да бъде минимум 5 (пет) години, считано от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.*

5. Място на изпълнение

5.1. Потвърждаваме, че мястото на извършване на доставката е на територията на гр. София, като сме запознати, че ще бъде посочено в писмената заявка конкретния адрес на извършване на доставката.

5.2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталиран софтуер.

6. Други изисквания

6.1. Декларираме, че сме надлежно упълномощени да извършваме доставка и гаранционно обслужване на предлагания от нас софтуер, необходим за обновяване на информационни и комуникационни системи на територията на Република България.

За удостоверяване на горното представяме **Официално оторизационно писмо от производителя MICRO FOCUS** (моля, посочете описание на документа)

Забележка: *За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлагания софтуер. Горепосоченият документ се представя в техническото предложение на участника.*

В случаите на представяне от участника на оторизационно писмо от официален представител на производителя (или еквивалентен документ), в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлагания софтуер.

6.2. Прилагаме **Общи условия за гаранционно обслужване от производителя на софтуера, предмет на обществената поръчка; Общи условия за организация на доставките и гаранционно обслужване от фирма СИЕЛА НОРМА АД; Продуктови брошури.**

Дата на подписване:	**10/07/2020 г.**
Подпис и печат:	.....
Име и фамилия	**Веселин Тодоров**
Длъжност	**Изпълнителен директор**
Наименование на участника	**Сиела Норма АД**

ОБЩИ УСЛОВИЯ

за организация на доставките и гаранционно обслужване от фирма СИЕЛА НОРМА АД

Доставката на хардуерни и софтуерни продукти се извършва съгласно условията и реда за осъществяване на доставката на оборудването, предвидени в договорите с нашите клиенти. Пет работни дни преди доставката ние уведомяваме клиентите си по електронна поща за детайлите на доставката, както и изпращаме списък на оборудването и техническата документация, които ще бъдат доставени. Хардуерните устройства и софтуерните продукти са винаги нови и неупотребявани, доставени в оригинални опаковки на производителя, с ненарушена цялост, окомплектовани с всички необходими интерфейсни и захранващи кабели, както и с необходимата техническа документация, на хартиен и електронен носител. Хардуерните устройства и софтуерните продукти, предмет на доставките ни, не са спрени от производство към датат на доставката и са включени в актуалните продуктови листи на производителя.

Предлаганите хардуерни устройства и софтуерни продукти отговарят на всички изисквания и стандарти на Република България, относно ергономичност, пожаробезопасност, норми за безопасност и включване към електрическата мрежа. Всички необходими актуални драйвери от производителя се предоставят на електронен носител заедно с хардуерните устройства и софтуерните продукти.

Гаранционният срок на хардуерните устройства и софтуерните продукти е в съответствие със закупеното ниво на техническа поддръжка и започва да тече от датата на приемо-предавателния протокол за доставка.В рамките на гаранционния срок ние се задължаваме да отстраняваме всички повреди и/или несъответствия, в т.ч. подмяна на дефектирали части, модули, устройства и/или компоненти с нови, съгласно гаранционните условия, както и обновяване на всички версии на софтуерните продукти. Всички заменени компоненти са с партиден номер на производителя.

Клиентът има възможност да изпрати всяко рекламационно съобщение по следните начини:

- телефон: 02/ 9030000
- електронна поща:ciela@ciela.com
- на адрес: гр. София, пк 1510, район Подуяне, бул. „Владимир Вазов“ № 9

Режимът на гаранционното обслужване е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч.

Ние осигуряваме преглед на място на техническите средства в обхвата на поръчката от наши квалифицирани представители в срок не по-късно от следващия работен ден, след получаване на рекламационно съобщение от клиента. След преглед се съставя констативен протокол за вида на повредата и/или несъответствието, както и дейностите и срока, необходими за отстраняването. Протоколът се подписва от представители на двете страни. Ние поемаме ангажимент да отстраним настъпила повреда и/или несъответствие и да възстановим пълната работоспособност на техническите средства, оборудвания и устройства на място при клиента. За извършените дейности по гаранционно сервизно обслужване предоставяме протокол, който съдържа описание на извършеното, подписан от представители на двете страни. Предоставяме и обобщен отчет в края на всяко тримесечие, както и в края на срока на договора с клиента.

Дата: 13.07.2020 г.

Подпис и печат.....

Веселин Тодоров, Изпълнителен директор

ОБЩИ УСЛОВИЯ

за гаранционно обслужване от производителя **MICRO FOCUS**

на продуктите, предмет на обществената поръчка **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите'', по Обособена позиция № 8: „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“**

Производителят **MICRO FOCUS** доставя своите софтуерни продукти със Бизнес ниво на поддръжка (**Micro Focus Business Support**). Бизнес нивото на поддръжка осигурява софтуерна поддръжка от типа **24x7x365**. **Времето за реакция** при критични проблеми е **до един бизнес ден.**

Бизнес поддръжката включва следните три основни компонента:

- 24x7 достъп до онлайн портал с помагала за извършване на самоподдръжка (Online Self-Service Support), който предоставя:
  - Достъп до обновления на софтуерните продукти на производителя и възможност за получаване на известия чрез електронна поща при пускане на нови версии;
  - Достъп до богата база от документация (ръководства, техническа документация, информация за справяне с познати проблеми) за софтуерните продукти на производителя;
  - Предоставяне на списък със закупените софтуерни продукти, които са обект на Бизнес поддръжката от производителя;
- Достъп до обновления на софтуерните продукти на производителя за периода на поддръжката и възможност за получаване на известия чрез електронна поща при пускане на нови версии:
  - Достъп до основни (major) обновления на софтуерните продукти на производителя, включващи нови или значително подобрени функционалности;
  - Достъп до минорни (minor) обновления на софтуерните продукти на производителя, с малки корекции или подобрения;
- Достъп до техническа поддръжка от квалифицирани кадри на производителя, която обхваща:

- Възможност за докладване на неограничен брой технически проблеми и неизправности, свързани със закупените софтуерни решения, за преглед от техническия екип на производителя;
- Обратна връзка от техническия екип по докладваните технически неизправности и въпроси. Възможност за комуникация по няколко канала: електронна поща, чат, телефонно обаждане;
- Техническата поддръжка от производителя се поддържа на няколко езика: английски, китайски, френски, немски, италиански, японски, португалски, испански. Техническа поддръжка извън стандартните бизнес часове се предоставя единствено на английски език;
- Предоставяне при необходимост от производителя на временни лицензионни ключове за софтуерните продукти, ако някоя от стъпките за отстраняване на техническа неизправност ги изсиква;

Времената за реакция на техническия екип на производителя при подаване на информация за технически неизправности, при Бизнес поддръжка с достъпност тип 24x7x365, са както следва:

- За инциденти от степен 4 – минорни инциденти, които не водят до прекъсване на процеси и услуги на софтуерните продукти – отговор до 1 бизнес ден;
- За инциденти от степен 3 – средни или минорни инциденти, които водят до кратко прекъсване или неизправност на процеси и услуги на софтуерните продукти – отговор до 6 часа;
- За инциденти от степен 2 – големи инциденти, които водят до сериозно ограничаване или прекъсване на процеси и услуги на софтуерните продукти, но не спиращи изцяло работния процес на организацията – отговор до 3 часа;
- За инциденти от степен 1 – критични инциденти, които водят до трайно прекъсване на процеси и услуги на софтуерните продукти и спиране на работния процес на организацията – отговор до 1 час;

Повече информация има на следния адрес:
https://www.microfocus.com/media/documentation/micro_focus_business_support_agreement.pdf

Дата: 13.07.2020 г. Подпис и печат.....

Превод от английски език:

Лого на Майкро Фокус (MICRO FOCUS)

юни 2020

ПИСМО ЗА УПЪЛНОМОЩАВАНЕ

Уважаеми господа,

С настоящото потвърждаваме, че Майкро Фокус е информирана, че **Сиела Норма АД**, с официален адрес: бул. „Вл. Вазов" № 9, 1510 София, България (наричана по-нататък "Участник в търга"), понастоящем упълномощен продавач на Майкро Фокус, ще подаде оферта до **Информационно обслужване АД**, с официален адрес: ул. „Панайот Волов" № 2, 1504 София, България, за търг №: 05948-2020-0004 / Доставка на комуникационно оборудване, хардуер и софтуер, необходими за осъвременяване и обновяване на информационните и комуникационни системи на Националната агенция за приходите.

Майкро Фокус потвърждава, че **Сиела Норма АД** е партньор на Майкро Фокус, упълномощен да доставя продуктите и услугите на Майкро Фокус в България през финансовата 2020 г.

С настоящото писмо разширяваме обхвата на упълномощаване, за да извършват гаранционното обслужване на системите. Участникът в търга ще предоставя пълната ни гаранция относно предлаганите и доставени от него продукти в съответствие с нашите Условия за крайния потребител.

В рамките на горецитирания проект и възможния последващ договор, Участникът в търга действа самостоятелно и от свое име. Участникът в търга не е нито служител, нито представител на Майкро Фокус.

С уважение:
Маруан Шанти
Директор по международни въпроси
Майкро Фокус
(подпис)

Фирмена бланка: Майкро Фокъс, офис в Обединеното кралство The Lawn, 22-30 Бат Роуд, Нюбъри, Бъркшър RG14 1QN, Обединено кралство, +44 (0) 1635 32646, +44 (0) 1635 33966, microfocus.com

Долуподписаната Деница Даковска, вписана под № 01250-1 към МВнР в Списъка на физическите лица, извършващи преводи, удостоверявам верността на извършения от мен превод от английски на български език на приложения документ: ....

Пр
Пр
(собственоръчно изписани обаче имена на преводача)

June 2020

Authorization letter

Dear Sirs,

This is to confirm that Micro Focus is aware that **Ciela Norma AD.**, legal address: 9 Vl.Vazov Blvd, 1510 Sofia, Bulgaria(herein "the Bidder"), presently a Micro Focus authorized reseller, shall submit a bid to **Information Services AD**, legal address: #2 Panayot Volov Str, Sofia 1504, Bulgaria for the tender number: 05948-2020-0004 / Supply of communication equipment, hardware and software for upgrade and renovation of information and communication systems of the National Revenue Agency

Micro Focus confirms that **Ciela Norma AD** is a Micro Focus partner authorized to deliver Micro Focus products and services in Bulgaria for the duration of Financial Year 2020.

We hereby extend their authorization to perform the warranty service of the systems. The Bidder will provide our full guarantee and warranty for the products offered and supplied by them in accordance with our End User Terms.

In the framework of the above-mentioned project and its possible subsequent contract, the Bidder is acting on its own name and behalf. The Bidder is neither an agent nor a representative of Micro Focus.

Sincerely,

Marwan Shanti

Channel Director

International

Micro Focus

ВЯРНО С ОРИГИНАЛА

Micro Focus
UK He
The Lawn, 22-30 Old Bath Road
Newbury, Berkshire
RG14 1QN, UK
+44 (0) 1635 32646
+44 (0) 1635 33966
microfocus.co

NetIQ SecureLogin

SecureLogin е един от водещите продукти за еднократно вписване (SSO) на пазара днес. Той позволява на потребителите да имат достъп до локални и мрежови ресурси, като използват единен набор от идентификационни данни. Когато потребителите се вписват в декстоп работна станция, SecureLogin автоматично ги удостоверява във всички свои приложения и ресурси. Само с една парола, която да запомнят, потребителите вече не трябва да ги записват; да създават слаби пароли, за да ги запомнят лесно, или да се обаждат на екипа по поддръжката за възстановяване на паролите, когато ги забравят.

Акценти на продукта

Основни предимства

NetIQ® SecureLogin Ви помага да облекчите проблемите с паролите на крайните потребители и същевременно помага на крайните потребители да се съсредоточат върху основната си работа, като по този начин повишава производителността на Вашите служители. Със SecureLogin не само получавате възможност за еднократно вписване за всичките си приложения в Windows, но и допълнителното предимство да можете да добавяте други фактори за идентификация, когато това наистина е необходимо. Вие избирате кои приложения не трябва да изискват допълнителна идентификация след като потребителят вече се е идентифицирал веднъж, Вие също така избирате кои приложения да изискват допълнителна идентификация. Това Ви дава свободата да проектирате своя собствена схема за идентификация на потребителя и да не бъдете ограничени до това, за което приложението е проектирано.

SecureLogin също така помага за намаляване на обажданията до отдела за поддръжка, като предоставя гъвкавост на крайните потребители да управляват собствените си профили и пароли.

SecureLogin позволява споде[illegible] работни станции да се използват като киоск-системи, което позволява на потребителите с едно натискане на бутон бързо да се вписват и директно да достигнат до желаното от тях приложение. След като е приключил работата си, потребителят може да се отпише от системата отново просто с едно натискане на бутон.

Основни функции

■ **Еднократно вписване за всички приложения на Windows.**
Поддържат се всички видове приложения за Windows, вариращи от .NET, Java, основани приложения и уеб приложения на всички популярни браузъри. Напълно с безпроблемна работата[illegible] на крайните потребители, като им се помага да се съсредоточат върху основната си работа.

■ **Поддръжка на отдалечени потребители**
Еднократно вписване, което работи дори когато потребителят не е свързан. SecureLogin запазва локален кеш за всички приложения на потребителите и им помага дори когато нямат достъп до данните.

■ **Поддръжка на Advanced Authentication метод за вписване**
Когато се използва Advanced Authentication, SecureLogin може не само да помогне да се заменят паролите с други методи за идентификация, но и да [illegible]

ET „Л и С - Стилияна Махалджийска"
Офис „Изток": 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1": 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора
Офис „Бизнес парк София": 1715 София, Бизнес парк София, сграда 8, вх. А - Б, т
ET „L&S - Stiliyana Mahaldjiiska"
Office „Istok": 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1": 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia": 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55
[illegible]ante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

ниво на удостоверяване в случай на достъп до критични приложения или данни.
Поддържат се повечето смарт карти, proximity карти и устройства за идентификация с токени или биометрични данни, както и много други методи.

■ **Бърза превключване на потребителски акаунти**
При сценарии на използване от тип киоск-система или при използване на споделена работна станция, на потребителите може да им потрябва само бързо да влязат, за да си свършат работата и след това да превключат към досегашния им режим на работа. Това гарантира, че когато се появи следващият потребител, предишният потребител се е отписал от използваната временно система. Администратора на решението и конфигурираното от него конкретно приложение, за автоматични действия когато се впише даден потребител, помага на потребителя да изпълни своите задачи много бързо. Това помага на потребителите да се движат между крайните устройства бързо и сигурно.

■ **Самообслужване за промяна на парола**
Това помага на потребителите да променят паролите си, да променят данните на потребителския си профил и да преглеждат достъпните ресурси на организацията, без да се нуждаят от помощ от отдела за поддръжка.

■ **Автоматизация на приложения**
SecureLogin поддържа използването на скриптове, които могат да Ви помогнат да автоматизирате много интерфейси на приложения. Администраторите могат да пишат скриптове, които могат да автоматизират действия с потребителски интерфейс на приложения, които биха могли да им помогнат да създадат по-интелигентни работни процеси.

■ **Управление на идентичността**
Възможност за интеграция с всяко решение за управление на идентичност, за да се помогне за автоматизирането на осигуряването на потребител, който трябва да бъде добавен или изключването на потребител, който е отстранен или променя ролята си.

■ **Лесно вписване в съществуващата архитектура, без изисквания за премахване и подмяна на данните за вписване**
SecureLogin използва съществуващата Ви инфраструктура за идентичност като своя локация за съхранение на данни. Той може да съхранява всичките си данни във всяка директория, съвместима с LDAP. Така че не е необходимо да добавяте, да премахвате или заменяте някоя част от Вашата инфраструктура.

■ **Помощник за обучение по процесите за еднократно вписване (SSO)**
SecureLogin се предлага с вграден софтуерен помощник, който Ви помага да обучите на SSO всяко приложение автоматично. Този помощник е много лесен за използване и сам разпознава параметрите на изискваната от дадена система парола. Всичко необходимо, за да работи, е да му се зададе от администратор на решението какви действия трябва да се предприемат на екрана.

Бърз преглед на решението

■ Лесно се вписва в съществуваща архитектура без изисквания за премахване и подмяна на данните за вписване
■ Интегрирайте приложенията бързо с помощта на вграден съветник за интеграция.
■ SSO както в Windows, така и в уеб базирани приложения
■ Винаги предоставяйте SSO при преносими устройства, дори когато те не са свързани
■ Поддръжка на Advanced Authentication механизми
■ Бързо превключване на акаунтите на потребителите за работни станции тип киоск-система
■ Самообслужване за промяна на парола
■ Мощен софтуер за автоматизация, който може да предостави много повече от просто извеждане на екрани с пароли
■ Разширена идентификация за конкретни приложения
■ Citrix сертифициран
■ VMware сертифициран
■ Поддържат се терминални сървъри на Windows

■ Интегрира се с решения за управление на идентичността, за да осигури автоматизация на работния процес

Системни изисквания

Поддържани клиенти:
■ Windows 7, Windows 8 и Windows 10.
■ Windows Server 2008 R2, 2012 и 2016
■ Клиент на Citrix Win32 ICA
■ Клиент на Windows Terminal Services, RDP
■ VMware VDI

Поддръжани уеб браузъри:
■ Internet Explorer
■ Mozilla Firefox
■ Google Chrome
■ Microsoft Edge

Поддържани типове Directory Server:
■ Microsoft Active Directory
■ Microsoft Active Directory Lightweight Directory Services (LDS)
■ Приложение Microsoft Active Directory Mode (ADAM)
■ NetIQ eDirectory ™
■ LDAP директории, съвместими с V3, работещи на която и да е от следните платформи:
■ Microsoft Windows Server
■ Sun One
■ Citrix Presentation Server
■ Citrix XenApp

Поддържани хранилища на данни за вписване:
■ Microsoft LDS, ADAM, терминален сървър или разширен сървър с Active Directory
- Microsoft Windows Server или терминален сървър с Active Directory
- Open Enterprise Server с NetIQ eDirectory
- NetIQ eDirectory на OES на поддържаните платформи
■ Сървъри използващи съвместими LDAP директории

„Ние се чувстваме готови за бъдещето с нашето решение от Micro Focus® и оценяваме, че специалистите от Micro Focus отделиха време, за да разберат нашите изисквания, както сега, така и за в бъдеще, като работят съвместно с нас, за да намерят най-доброто и най-рентабилното решение за нас."

Йорген Сандстром
Ръководител на отдел дигитализация
SKL

Подписаната, [redacted] *ЕГН:* [redacted], *Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ , извършен от мен. Преводът се състои от* 4 *страници.*

Подпис: [redacted]

ЕТ "ЛиС - Ст. Мahaldjiiska" * София * L&S * ЕТ "ЛиС - Ст. Махалджиска"

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

MICRO FOCUS

Data Sheet
Security

NetIQ SecureLogin

SecureLogin is one of the leading single sign-on (SSO) products on the market today. It allows users to access local and network resources using a single set of credentials. When users log into a desktop, SecureLogin automatically authenticates them to all of their applications and resources. With only one password to remember, users no longer need to write them down; create ones that are weak so they're easy to remember, or call helpdesk for resets when they forget them.

Product Highlights

Key Benefits

NetIQ® SecureLogin helps you to ease out the password pains for end users and helps them focus on their primary job thereby increasing the productivity of your employees. With SecureLogin not only do you get single sign on ability for all your applications on Windows but also an added advantage of being able to add other factors of authentication where it is really needed. You choose which applications need not ask for authentication after the user has already authenticated, you also choose which applications require a step up. This gives you the freedom to design your own flow of user validation and not be restricted to what an application is implemented to do.

SecureLogin also help reduce helpdesk calls by giving the flexibility to the end users to manage their own profiles and passwords.

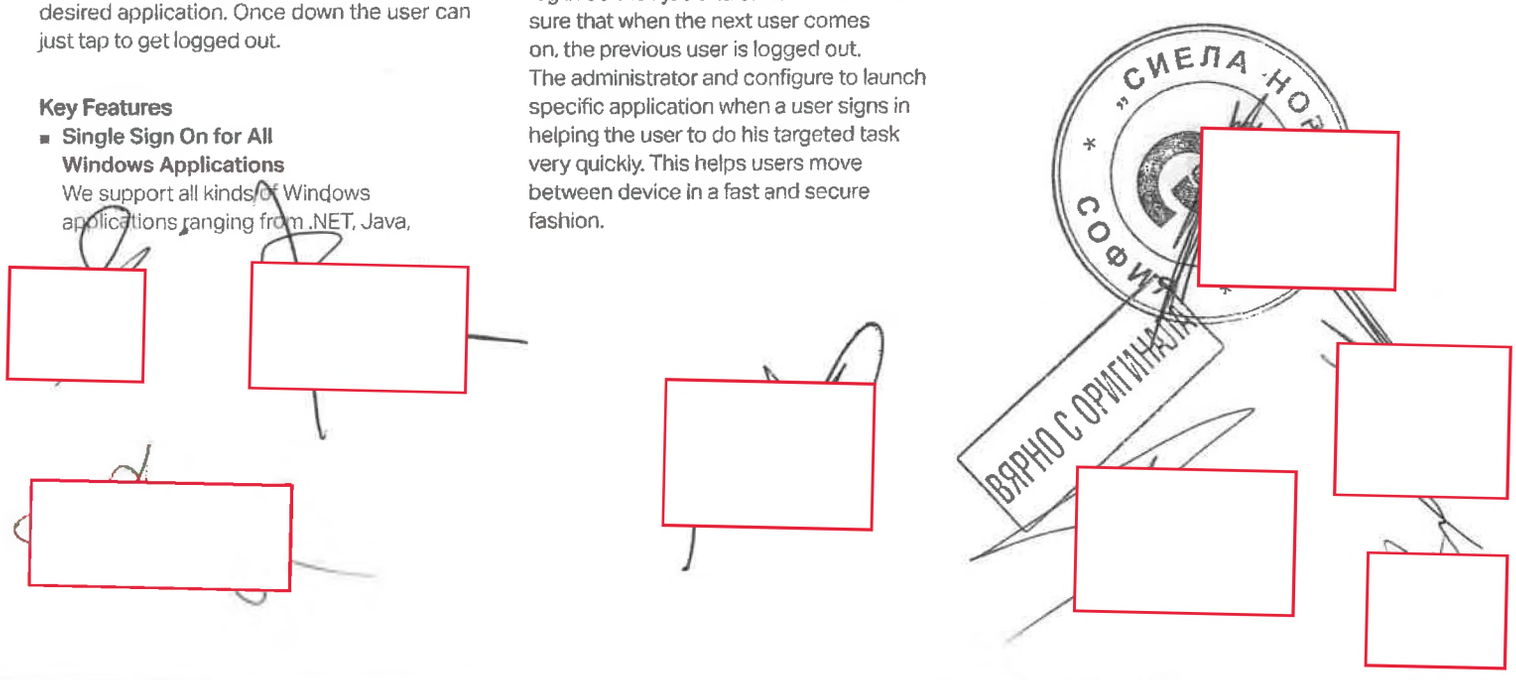
SecureLogin enables shared workstations to be used as kiosks enabling users to quickly tap in to get logged in and directly land onto the desired application. Once down the user can just tap to get logged out.

Key Features

- **Single Sign On for All Windows Applications**
  We support all kinds of Windows applications ranging from .NET, Java, native applications to web applications on all popular browsers. It is completely seamless for end users, helping them focus on their primary job.
- **Remote Users Support**
  Single sign that works even when the user is not connected. SecureLogin keeps a local cache for all the applications of the users and helps them even when it is not able to access the data.
- **Advanced authentication supports**
  When deployed with Advanced Authentication, SecureLogin can not only help replace passwords with other methods of authentication but also do a step up authentication in case critical applications or data is being accessed. We support most smart cards, proximity cards and token based or biometric authentication device and many other methods.
- **Fast user switching**
  In kiosk or shared workstation kind of scenarios, users might need to swiftly log in do their job and switch. This makes sure that when the next user comes on, the previous user is logged out. The administrator and configure to launch specific application when a user signs in helping the user to do his targeted task very quickly. This helps users move between device in a fast and secure fashion.

Quick View

- Easily fits into existing architecture with no rip-and-replace requirements
- Integrate applications quickly using a built-in integration wizard.
- SSO experience across both Windows and web based applications
- Always provide a SSO experience for portable devices, even when they are not connected
- Advanced authentication supports
- Fast user switching for kiosk based workstations
- Self-service password reset
- Powerful automation engine that can do much more than just password screens
- Step up authentication for specific applications
- Citrix Certified
- VMware Certified
- Windows terminal servers supported
- Integrates with Identity management solutions to provide workflow automation



"We feel ready for the future with our Micro Focus® solution and appreciate that Micro Focus took the time to understand our requirements, both now and in the future, and worked with us to find the best and most cost effective solution for us."

JORGEN SANDSTROM
Head of Section Digitization Division
SKL

Contact us at:
www.microfocus.com

Like what you read? Share it.

- **Self-service password reset**
  This helps users reset their passwords, change their profile data and browse the company white pages without needing help from a help desk.
- **Application Automation**
  SecureLogin has a scripting framework that can help you automate many application screens. Administrators can write scripts that can automate UI actions on applications which could help them create smarter workflows.
- **Identity management**
  We can integrate with any identity management solution to help automate provisioning of a user who needs to be on-boarded or de-provisioning for a user who is exiting or changing the role.
- **Easily fits into existing architecture with no rip-and-replace requirements**
  SecureLogin uses your existing identity infrastructure as its data store. It can store all its data in any LDAP compliant directory. So there is no need to have an additional, remove or replace any of your infrastructure.
- **Wizard for SSO training**
  SecureLogin comes with a built in wizard that help you train it to SSO any application. This wizard is very easy to use and recognizes a password form on its own, all we need to do is tell it what actions it needs to take on the screen.

System Requirements

Clients Supported:
- Windows 7, Windows 8 and Windows 10.
- Windows Server 2008 R2, 2012 and 2016
- Citrix Win32 ICA Client
- Windows Terminal Services Client, RDP
- VMware VDI

Web Browser Support:
- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Directory Server Support:
- Microsoft Active Directory
- Microsoft Active Directory Lightweight Directory Services (LDS)
- Microsoft Active Directory Application Mode (ADAM)
- NetIQ eDirectory™
- V3-compliant LDAP directories, operating on any of the following platforms:
- Microsoft Windows Server
- Sun One
- Citrix Presentation Server
- Citrix XenApp

Credential Repository Servers:
- Microsoft LDS, ADAM, Terminal Server, or Advanced Server with Active Directory
  - Microsoft Windows Server or Terminal Server with Active Directory
  - Open Enterprise Server with NetIQ eDirectory
  - NetIQ eDirectory on OES on supported platforms
- Servers running LDAP-compliant directories

MICRO FOCUS

Identity Manager: Основата за управление и администриране на идентичности

Micro Focus® Identity Manager предлага цялостно, но достъпно решение за контрол на това кой има достъп до това, което се намира във Вашето предприятие - както в локалната мрежа зад защитната стена, така и в облака.

Кратко представяне на Identity Manager:

Identity Manager е проектиран да управлява целия жизнен цикъл на идентичностите по модулен, но интегриран начин, така че да можете да адресирате настоящите и бъдещите си потребности, когато такива възникнат.

С развръстването идват усложненията и предизвикателствата пред сигурността

Когато предприятията се развиват, те са непрекъснато предизвикани да осигурят навременен достъп до нови приложения и услуги. С бързото навлизане на устройствата, лесния достъп, осигурен от пазарното развитие на ИТ, и свързаността навсякъде, където се намирате, предприятията са изправени пред предизвикателството да удовлетворят потребностите на потребителите на работното място, като същевременно поддържат адекватно управление на достъпа до приложения и данни. Предприятията прилагат различни процеси, за да се справят с това предизвикателство, но за да бъдат успешни, стабилното и ефективно управление на идентичностите е основополагащо, за да се осигури гъвкавост, необходима за адаптиране към променящите се бизнес нужди.

Постоянната свързаност се е превърнало в норма, работното място вече е навсякъде и предпочитанията на бизнес потребителите се към интерфейсите на мобилните устройства. Потребителите се чудят: „Защо не мога да имам достъп до това, от което се нуждая сега?“ или „Защо не мога просто да изтегля приложение?“ и „Защо ме питат за друга парола?“. Тези тенденции на потреблението насочени към удобство диктуват избора на технологии.

Съпоставимо, ако не и по-голямо предизвикателство, е осигуряването на защита на корпоративните активи, данни и съответствието с вътрешни и външни регулации. Предотвратяването на неоторизиран достъп до чувствителна информация е изключително трудно, когато облачните приложения и мобилните устройства са извън контрола на ИТ.

Постигането на баланса между лекотата на използване и адекватните контроли може да бъде сложна задача. За да отговори на тези предизвикателства, Вашата организация се нуждае от цялостно решение, което управлява идентичностите на потребителите и свързаните с тях атрибути в различни приложения. Тези приложения могат да бъдат локални, доставени от партньори или софтуер като услуга. Решението за управление на идентичностите поддържа подходящи права за достъп и може да обогати данните за сигурност, за да разбере как и кога потребителите използват корпоративните активи. Стратегическият подход на Micro Focus за управление и администриране на идентичности (IGA) идентифицират и блокират процесите, които излагат Вашата

организация на риск, като задоволява разнообразните потребности на Вашите потребители - от служители до клиенти.

Identity Manager предоставя цялостен подход към сложните изисквания
Identity Manager поддържа целия жизнен цикъл на управление на идентичностите и свързаните с тях атрибути, за да минимизира привилегиите. Това дава възможност на Вашата организация да намали разходите за ръчно управление на акаунти и да постигне съответствие с наложените регулации, като същевременно намалява риска от неоторизиран достъп. Решението предоставя ползи за всички критични заинтересовани страни във Вашата организация. Например, то позволява на Вашия:

- ИТ Директор да намали разходите за спазване на изискванията и да предложи по-удобен достъп, така че бизнесът да може да се възползва от новите възможности
- Главен директор по сигурността на информацията да наложи спазване и защита на достъпа в целия бизнес процес
- Бизнес мениджърите да поддържат екипите си продуктивни, като осигуряват незабавен, базиран на роли достъп до ресурси
- ИТ мениджърите да управляват по-добре ресурсите и да предоставят подробни данни за използваните идентичности на основните заинтересовани страни

Identity Manager е проектиран да управлява целия жизнен цикъл на идентичностите по модулен, но интегриран начин, така че да можете да адресирате настоящите и бъдещите си потребности, когато те се появят. Възможностите включват:

Управление на създаването и анулирането на акаунти, както и промените произтичащи от смяната на работната позиция на даден служител: Identity Manager предлага интегрирани функции за управление на работни процес, базирани на роли-правила, които осигуряват най-ефективното решение на пазара днес. Автоматизирайте толкова, колкото има смисъл за Вашата организация. Софтуерът съответства на начина, по който работи Вашата организация, като комбинира бизнес правила с ефективността на незадължителното предоставяне на роли, което позволява на софтуера да се справя със стандартни одобрения и изключения като например конфликти при разделяне на отговорностите.

Управление на идентичностите и промените в правата за достъп в предприятието: Identity Manager използва архитектура, базирана на събития, и прилага правомощия за идентичност във всички свързани системи, като гарантира, че идентичностите се създават само от подходящи източници. Освен това Identity Manager налага привилегии, което означава, че системи, които „притежават" компоненти на идентичността са единствените, които могат да ги променят, и ако се променят в неавторитетни източници, те могат да бъдат автоматично пренастроени на стойността в авторитетния източник. И двете са критични, когато основните провизии и политиките за предоставяне и достъп са базирани на атрибути.

Поради способността за реагиране в реално време, когато се случи събитие от жизнения цикъл на потребителя (т.е. наемане, промяна на ролята, уволнение), механизмът за управление на данни на Identity Manager може да задейства автоматизирани процеси, базирани на политики.

Освен това, различни приложения, като Microsoft SharePoint и SAP системи, имат свои собствени методи за налагане на политики. Identity Manager улеснява интегрирането на различни права в консолидиран каталог, използвайки услугата за съгласуване на ресурси на Identity Manager.

Тази способност Ви позволява автоматично да откривате разрешения и да използвате визуални операции за картографиране на ресурси към подходящи роли или ресурси на Identity Manager.

Безпроблемното интегриране на различни методи за налагане на политики в една система бързо създава единен управляващ механизъм, който дава на правилните индивиди пълен поглед върху привилегиите на потребителите и им дава възможност да вземат информирани решения за оценка на рисковете и гарантиране на това правилните хора да имат достъп до правилните ресурси. Не само е лесно за първоначална настройка, но и продължителната поддръжка от производителя предоставя на Вашата организация гъвкава система за управление на ресурси и права във всички свързани системи, независимо къде се намират те - в локалната мрежа или в облака.

Designer for Identity Manager предлага възможност за създаване на работни потоци за заявка за достъп, които могат драстично да намалят човешките грешки, без да се изисква програмиране или персонализиране. В графичния интерфейс Вашите администратори могат да управляват целия жизнен цикъл на проекта, включително да проектират и симулират различни конфигурации за управление на акаунти без никакви скриптове. Докато добавяте все повече управлявани от Identity Manager приложения в цялата Ви среда, предизвикателството за „почистване на данни“ може да отнеме много време.

Analyzer for Identity Manager, функция в Designer, ефективно показва и сравнява данни от хранилището за съхранение на идентичности, както и в свързани системи, като намалява времето, необходимо за подготовката на приложенията за интегриране в инфраструктурата за идентичности, като по този начин намалява времето и разходите, необходими за свързване на нови системи.

Процес за заявка и одобрение за достъп на потребителя на принципа на самообслужване: Използвайки интуитивен, удобен за бизнеса графичен интерфейс, бизнес потребителите могат да правят и проследяват заявки за достъп и да управляват задачи за одобрението им от едно място. Тази възможност за самообслужване дава на потребителите контрол върху собствената им информация за идентичност, така че те могат да останат продуктивни, като същевременно намаляват натоварването на ИТ за обработка на заявки. Пълната интеграция със системата за сигурност означава, че потребителите могат да получат необходимия им достъп почти веднага, вместо да чакат ръчно изпълнение.
Одобряващите обикновено са бизнес мениджъри, които пътуват по работа и са в движение. Производителността се губи, когато заявките от потребителите трябва да изчакат одобрителя да бъде в офиса. В днешния свят работата е дейност, а не местоположение.
Приложението за мобилно одобрение на Identity Manager е собствено и сигурно мобилно приложение, което може лесно да се инсталира на всяко мобилно устройство, което позволява на одобряващите да бъдат незабавно сигнализирани и да отговарят на искания от всякъде. Освен това има опции за делегиране, връщане или преназначаване на задачи.

Самообслужване за парола: Един от най-големите разходи за екипите по поддръжката са генерирани от помагането на потребителите да сменят или възстановят паролите си. Самообслужването за промяна на паролата (SSPR) може на практика да елиминира участието на екипите по поддръжката, като позволява на потребителите да управляват и променят собствените си пароли и дори да активират отново заключените акаунти, като същевременно поддържа сигурността, която Вашата компания изисква.
Със самообслужването за промяна на паролата потребителите потвърждават коя е тяхната идентичност, преди да получат разрешение защитено да променят паролите си. Който и метод да се избере за идентификация, се отразява подходящото ниво на сигурност, което Вашата организация изисква, а новите пароли винаги се придържат към изискванията при прилагането на правилата за парола при въвеждане. По този начин няма опасност да се замени силна парола с по-слаба, която не отговаря на посочените изисквания. Новите пароли и отключените акаунти са ефективни незабавно, така че потребителите могат да получат незабавен достъп до своите системи и приложения.

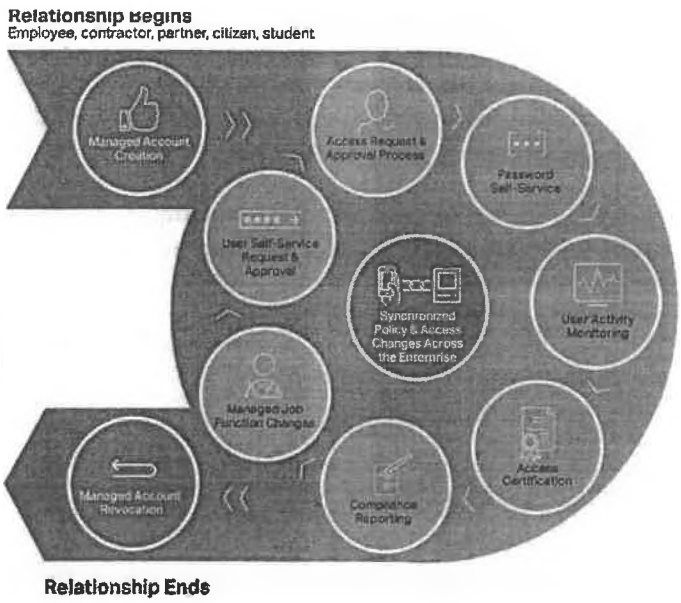
Наблюдение на потребителската активност: Знаейки и управлявайки кой има достъп до какво е само част от картината. Знанието какво правят хората с достъпа си - исторически и в реално време - е също толкова важно. Неволното допускане на несъответстващо, злонамерено или неправилно поведение може да доведе до огромни глоби, неуспешни одити и тежки щети на информационните бази и бизнес репутацията на Вашето предприятие.
Наличният Micro Focus Identity Tracking за Identity Manager съчетава мощните способности за информиране и предоставяне на идентичности на Identity Manager с механизъм за корелация в реално време, за да Ви даде пълна картина за това кой има достъп до какво и какво правят хората с техния достъп. Това решение за мониторинг и коригиране на дейностите на потребителя работи във всички системи, които защитава Identity Manager, като значително намалява рисковете от несъответстващо, злонамерено или неправилно поведение, носещо щети за Вашето предприятие.

Сертифициране на правата за достъп: Периодичните прегледи на правата за достъп са изискване за съответствие и могат да отнемат значително време. ИТ екпите губят време за събиране на права за достъп и са необходими много усилия на бизнеса за удостоверяване на тези права. Наличното Identity Governance решение се интегрира с Identity Manager и автоматизира голяма част от този процес, като дава възможност на организациите да преглеждат и сертифицират достъпа на потребителите до приложения и системи в предприятието, включително тези, управлявани от Identity Manager, както и тези, които не са. Управлението на идентичностите позволява преглед на управлявани и неуправлявани приложения, дава възможност за периодични или ad-hoc прегледи, позволява прегледи от супервайзър, поддържа прегледи както от собственици на приложения, така и от собственици на разрешения, опростява прегледите базирани на риска и изпълнява решенията за преглед автоматично или ръчно.

Отчети за доказване на съответствие: Identity Manager е оборудван с всеобхватни възможности за изготвяне на отчети, от които Вашата организация се нуждае, за да докаже съответствието на правата за достъп с наложените изисквания. Отчетите осигуряват не само видимост до кои системи в момента потребителите могат да имат достъп, но и до кои системи биха могли да имат достъп на определени дати или между два момента. Системата за отчети също така позволява на потребителите да създават персонализирани отчети, които да отговарят на техните специфични изисквания и да запазват отчетите за бъдеща употреба. Възможностите за събиране и съхранение на данни, основани на политиките, осигуряват силна подкрепа за спазване на съответствието, така че Вашата организация да е винаги готова за следващия си одит.

Заключение

Тестваното във времето и награждавано решение Micro Focus Identity Manager предлага цялостно решение за контрол на това кой има достъп до какво във Вашето предприятие – както локално разположени ресурси, зад защитната стена, така и в облака. То Ви позволява да осигурите сигурен и удобен достъп до критична информация за бизнес потребителите, като същевременно отговаряте на изискванията за съответствие. Можете да сте сигурни, че то разполага със сертификат Common Criteria от степен 3 (EAL3 +). Използвани от хиляди клиенти по целия свят, Micro Focus Identity Manager предоставя високо мащабируема, диференцирана основа за управление на идентичностите, като гарантира, че Вашата организация може да остане конкурентоспособна, пъргава и защитена - на ниска цена. То предлага интегриран подход за внедряване на решения за целия бизнес или индивидуални продукти за управление на идентичностите и достъпа, за да се отговори първо на най-належащите потребности. С нашите продукти и решения, Вашето предприятие получава най-високата стойност от своите минали, настоящи и бъдещи ИТ инвестиции.



Фигура 1. Жизненият цикъл на Identity Manager, поддържан от Micro Focus Identity Manager

Фигура 2. Identity Manager предоставя на потребителите персонализиран за бизнеса им графичен интерфейс, показващ информация за задачи, роли и заявки

„С централизирано управление на идентичностите на потребителите можем да управляваме нашата компания безпроблемно. Клиентите вече не трябва да помнят множество идентификационни номера и пароли, за да получат достъп до многото си услуги при нас. "
КАНОН КОЗАД
Старши вицепрезидент и директор за разработка на приложения.
UMB Financial Corp.

Подписаната, [redacted], ЕГН: [redacted], Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ , извършен от мен. Преводът се състои от 6 страници.

Подпис: [redacted]

[redacted]

MICRO FOCUS

Identity Manager: The Foundation for Identity Governance and Administration

Micro Focus® Identity Manager delivers a complete, yet affordable solution to control who has access to what across your enterprise—both inside the firewall and into the cloud.

Identity Manager at a Glance:
Identity Manager is designed to manage the complete identity lifecycle in a modular yet integrated manner so you can address current and future needs as they come.

With Growth Comes Complexity and Security Challenges

As enterprises evolve, they are constantly challenged to provide timely access to new applications and services. With the explosion of devices, ease of access brought on by the consumerization of IT, and connectivity everywhere you go, enterprises are challenged to meet the demand for a consumer experience at work while maintaining adequate management of access to applications and data. Enterprises implement various processes to handle this challenge, but to be successful, a robust and effective management of identity is foundational to provide the flexibility needed to adjust to changing business needs.

With constant connectivity being the norm, the workplace is now anywhere and business user preferences have shifted towards mobile device interfaces. Users wonder, "Why can't I have access to what I need now?" or "Why can't I just download an app?" and "Why am I being asked for another password?" These consumerization trends toward convenience are dictating technology choices.

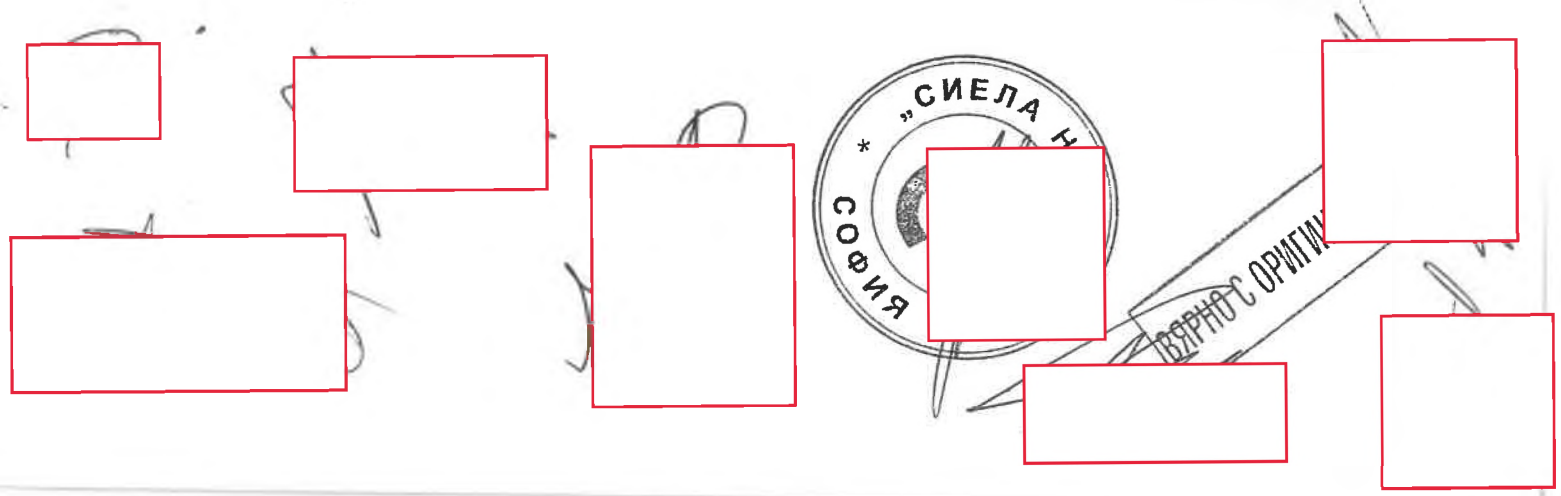
An equal, if not greater, challenge is ensuring the protection of corporate assets, data, and compliance with internal and external controls. Preventing unauthorized access to sensitive information is enormously challenging when cloud applications and mobile devices are outside of the control of IT.

Striking the balance of ease of use with adequate controls can be a formidable task. To answer these challenges, your organization needs a comprehensive solution that manages user identities and their associated attributes in various applications. Those applications may be on-premises, partner-delivered, or software as a service. An identity foundation supports appropriate access and can enrich security data to understand how and when users are using corporate assets. Micro Focus's strategic approach to Identity Governance and Administration (IGA) closes the loopholes that exposes your organization to risk, while satisfying the diverse needs of your users—from employees to customers.

Identity Manager Provides a Comprehensive Approach to Complex Requirements

Identity Manager powers the entire identity management lifecycle, managing identities and their associated attributes to minimize privileges. This enables your organization to reduce the costs of manual account management and demonstrate compliance while reducing the risk of unauthorized access. It delivers benefits for all critical stakeholders in your organization. For example, it allows your:

- CIO to decrease the costs of compliance and offer more convenient access, so the business can take advantage of new opportunities
- CISO to enforce enterprise-wide access compliance and security
- Line-of-business managers to keep their teams productive by providing immediate, role-based access to resources



- IT managers to better manage resources and provide identity-rich usage data to key stakeholders

Identity Manager is designed to manage the complete identity lifecycle in a modular yet integrated manner so you can address current and future needs as they come. Capabilities include:

Managed Account Creation, Revocation, and Job Changes: Identity Manager offers an integrated roles-rules-workflow engine that provides the most efficient solution on the market today. Automate as much or as little provisioning as makes sense for your organization. The engine matches the way your organization does business by combining business rules with the efficiency of optional roles-based provisioning, allowing the workflow engine to handle standard approvals and exceptions such as separation-of-duties conflicts.

Managed Identity and Access Changes across the Enterprise: Identity Manager leverages an event-based architecture and enforces identity authority across all connected systems, ensuring identities are created only from appropriate sources. Additionally, Identity Manager enforces attributes authority meaning systems that "own" components of the identity are the only ones that can change them, and if changed in non-authoritative sources, they can be automatically re-set to the value in the authoritative source. Both are critical when basing provisioning and access policies on attributes. Due to the real-time response capability, when a user lifecycle event occurs (i.e. hire, role change, termination), Identity Manager's data-management engine can trigger automated policy-based processes.

Additionally, various applications, such as Microsoft SharePoint and SAP systems, have their own policy controls. Identity Manager makes it easy to integrate different entitlements into a consolidated catalog, leveraging the Identity Manager resource reconciliation service. This capability allows you to automatically discover permissions and use visual operations to map resources to appropriate roles or Identity Manager resources.

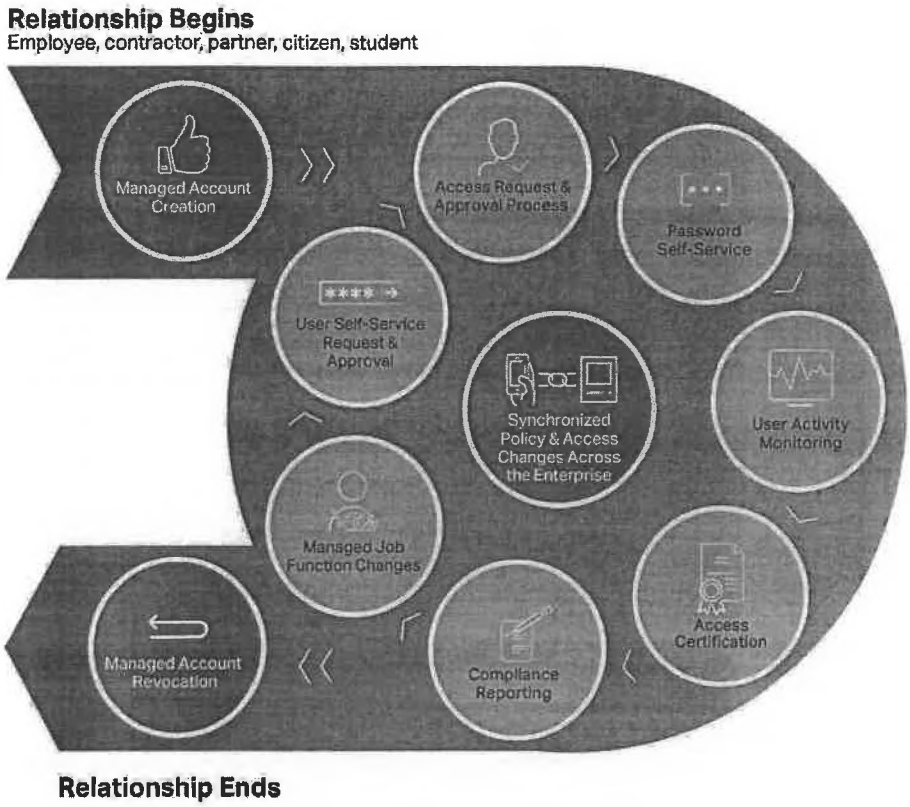


Figure 1. The Identity Management Lifecycle, Powered by Micro Focus Identity Manager

Seamlessly integrating different policy controls into one system quickly creates a unified governing mechanism that gives the right individuals a complete view of users' privileges and empowers them to make informed decisions to evaluate and ensure the right people have access to the right resources. Not only does it deliver ease-of-use for initial setup but ongoing entitlement maintenance provides your organization with an Agile system for managing resources and entitlements across all connected systems, no matter where the systems are located—on-premises or in the cloud.

Designer for Identity Manager offers the ability to produce access-request workflows that can dramatically reduce human error with no programming or customization required. In the graphical interface, your administrators can manage the entire project lifecycle, including designing and simulating various account management configurations without any scripting. As you expand Identity Manager to applications throughout your environment, the challenge of "data cleanup" can be time-consuming.

Analyzer for Identity Manager, a feature in Designer, efficiently displays and compares data from the identity vault and in connected systems, minimizing the time required to prepare applications for integration into the identity infrastructure, thereby minimizing the time and costs required to connect new systems.

User Self-Service Access Request and Approval Process: Using an intuitive, business-user friendly dashboard, business users can make and track access requests, and manage approval tasks all from one location. This self-service capability gives users control over their own identity information, so they can remain productive while reducing the workload on IT to handle requests. Full integration with the provisioning system means that users can get the access they need almost immediately, rather than waiting on manual fulfilment.

Approvers are typically business managers who travel for business and are on the go. Productivity is lost when requests from users have to wait on an approver to be in the office. In today's world, work is an activity not a location. The Mobile Approval Application for Identity Manager is a native and secure mobile application that can be easily installed on any mobile device allowing approvers to be immediately alerted and respond to requests from anywhere. Additionally, there are options for tasks to be delegated, returned or reassigned.

Password Self-Service: One of the largest helpdesk costs is borne by helping users reset their passwords. Self-service password reset (SSPR) can virtually eliminate the helpdesk's involvement by allowing users to manage and reset their own passwords and even re-enable locked accounts while still maintaining the security your company requires.

With self-service password reset, users confirm who they are through methods before they're allowed to securely reset their passwords. Whatever method is selected for identification reflects the appropriate level of security your organization requires, and new passwords always adhere to requirements with as-you-type password rule enforcement. That way, there's no danger of replacing a strong password with a weaker one that doesn't meet the specified requirements. New passwords and unlocked accounts are effective instantly, so users can gain immediate access to their systems and applications.

User Activity Monitoring: Knowing and managing who has access to what is only part of the picture. Knowing what people are doing with their access—both historically and in real time—is equally important. Inadvertently allowing noncompliant, malicious, or improper behavior could result in hefty fines, failed audits, and severe damage to your enterprise's information stores and business reputation. The available Micro Focus Identity Tracking for Identity Manager combines the powerful information and provisioning capabilities of Identity Manager with a real-time correlation engine to give you a complete picture of who has access to what and what people are doing with their access. This user-activity monitoring and remediation solution works across all systems that Identity Manager provisions, significantly reducing the risks of non-compliant, malicious, or improper behavior harming your enterprise.

Access Certification: Periodic access reviews are a compliance requirement and can consume significant time. IT wastes time compiling access entitlements, and too much effort is required of the business to certify those entitlements. The available Identity Governance solution integrates with Identity Manager and automates much of that process by enabling organizations to review and certify user access to applications and systems across the enterprise, including those managed by Identity Manager as well as those that are not. Identity Governance allows review of managed and unmanaged applications, enables periodic or ad-hoc reviews, allows supervisor reviews, supports both application and permission owner reviews, streamlines reviews based on risk, and fulfills review decisions automatically or manually.

Compliance Reporting: Identity Manager is equipped with the comprehensive reporting capabilities that your organization needs to prove access compliance. The reports not only provide visibility into which systems

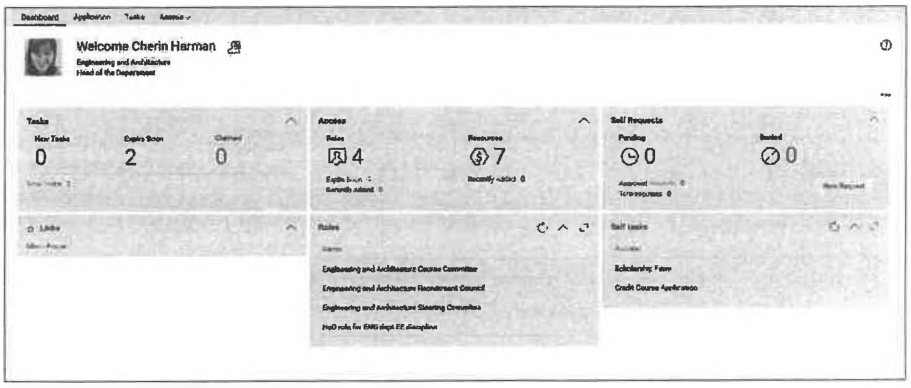


Figure 2. Identity Manager provides users with a customizable business friendly dashboard displaying information on tasks, roles and requests

"With centralized user identity management, we can present our company in a seamless fashion. Customers no longer need to remember multiple IDs and passwords to access their many different services with us."

KANON COZAD
Senior Vice President and Director of Application Development,
UMB Financial Corp.

Contact us at:
www.microfocus.com

users can currently access but also into which systems they could access on specific dates or between two points in time. The reporting framework also allows users to create custom reports to suit their specific requirements and to save the reports for future use. The policy-based data collection and storage capabilities provide strong compliance support so that your organization is always ready for its next audit.

Conclusion

The time-tested and award-winning Identity Manager delivers a complete solution to control who has access to what across your enterprise—both inside the firewall and in the cloud. It enables you to provide secure and convenient access to critical information for business users while meeting compliance demands. You can be confident in knowing that it has achieved Common Criteria Certification at Evaluation Assurance Level 3 with augmented assurance (EAL3+). Deployed by thousands of customers worldwide, Micro Focus delivers a highly-scalable, differentiated identity management foundation, ensuring your organization can stay competitive, agile, and secure—at low cost. It offers an integrated approach to deploying enterprise-wide solutions or individual identity and access management products to address the most pressing needs first. With our products and solutions, your enterprise gets the most value from its past, present, and future IT investments.

Access Manager

Micro Focus е водещ доставчик на уеб решения за еднократно вписване, които предоставят прозрачен и сигурен достъп до приложения и услуги. Поддържайки Federation стандартите за делегиране на права за достъп, NetIQ® Access Manager ™ дава възможност на организациите да споделят лична информация в мрежата, облака и чрез мобилни устройства сигурно и удобно. Тъй като предоставянето на сигурен достъп е повече от просто за този, който има нужда от него, Access Manager се адаптира към правилното ниво на идентификация на потребителя въз основа на измерения риск за бизнеса.

Представяне на продукта

Access Manager предоставя на потребителя еднократно вписване и сигурен достъп до вътрешната интранет мрежа и приложения, базирани в облак, от където и да се намира той: офис, отдалечен достъп, на път; или за клиентите, независимо от устройството, което използват. Access Manager прави това, като поддържа Federation стандартите за делегиране на права за достъп за съвременните приложения и услуги, като същевременно запазва най-добрите възможности за достъп за всичко останало. В допълнение към контрола за еднократно вписване и контрола на достъпа, Access Manager включва вграден софтуер, базиран на риска и двуфакторна идентификация, така че организациите да могат да поддържат лесен достъп, когато рискът е малък и да адаптират проверката на потребителя, когато рискът е висок или среден. Той е създаден да използва по-малко хардуер, да се внедрява по-бързо и да изисква по-малко поддръжка, като Ви предоставя по-бърз срок за възвръщаемост и по-ниски разходи за собственост.

За организации, които все още не разполагат с портал за достъп, Access Manager включва персонализирана страница за вход и портал за мини приложения, така че организациите да могат да ги маркират според нуждите си. Иконите на приложенията могат да се конфигурират и да се адаптират за средата, където се използват, като всичко това изисква минимално време и опит. Access Manager е изцяло проектиран за улеснение и ниска цена на собственост.

Основни предимства

Access Manager е подходящ за предоставяне на еднократно вписване и сигурен достъп до уеб-базирани приложения. С богатия си набор от функции, вградени адекватно в продукта, и с опростения си дизайн и интегриране с други решения за идентичност и контрол на достъпа на Micro Focus®, можете да избегнете сложното конфигуриране, асоциирано с подобен тип решения. Access Manager дава възможност на организациите да правят повече с по-малко, осигурявайки бърз и удобен достъп за потребителите, като същевременно запазва личната информация защитена. С Access Manager Вашата организация може да:

- Осигури сигурен достъп в цялата организация - Access Manager е пълно функционално решение за достъп, което предоставя еднократно вписване за модерни услуги, които поддържат SAML, WS-Federation, WS-Trust, OAuth и OpenID, както и приложения и услуги без Federation поддръжка.
- Постигнете бърз успех с Вашата мобилна стратегия - Независимо дали имате необходимост от еднократно вписване за своите вътрешно разработени корпоративни мобилни приложения или за вашите уеб приложения, Access Manager има

ET „Л и С - Стилияна Махалджийска“
Офис „Изток“: 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1“: 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в дво
Офис „Бизнес парк София“: 1715 София, Бизнес парк София, сграда 8, вх. А - Б
ET „L&S - Stiliyana Mahaldjiiska“
Office „Istok“: 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1“: 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02 974 57 55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55

решението. Той се предлага със SDK, който позволява федерация на приложения за разработчици, както и мобилен gateway, който осигурява достъп с един клик до legacy уеб приложения на мобилни платформи само за часове. Независимо от специфичния случай, можете да внедрите контрол за идентичност и достъп, без да докосвате back-end приложенията си. ■ Увеличете едновременно сигурността и удобството -

Access Manager има вграден механизъм за идентификация, базиран на риска, който позволява на организациите да адаптират процеса на идентификация на своя потребител въз основа на измерен риск, позволявайки на потребителите лесен достъп до среди с нисък риск и увеличаване на идентификация за ситуации с по-висок риск.

■ Интегрира се с други продукти за идентичност, достъп и защита на MicroMocus Focus, като по този начин дава възможност на организациите да предоставят удобен достъп на тези, които се нуждаят от него, като същевременно защитава организациите от тези, които не трябва да имат достъп, както отвътре, така и отвън.

Основни функции

Предприятията използват Access Management, за да интегрират достъпа до своите приложения и услуги във всички свои бизнес единици, независимо кой е собственик на хранилищата с потребителски данни. Federation и Gateway функциите му позволяват да свържете заедно облачните и интранет приложенията с безпроблемно единично регистриране и достъп.

■ Пълна поддръжка за Federation имплементации, използвайки SAML, OAuth, OpenID Connect, WS-Federation и други

■ Дизайнерът на потребителски интерфейс за страници за вход и портал позволява персонализирано брандиране и конфигурация на икони

■ Опция за използване на виртуално устройство, независимо какъв хипервайзор се използва (внедряване в почти всяка среда)

■ Интеграция по подразбиране с Microsoft SharePoint и Office 365 Enterprise

■ Пакет за разработка на софтуер за iOS устройства

■ Вградени функции за идентификация, базирана на риска, която осигурява оценка на риска и селективна идентификация въз основа на резултата

■ Интеграция по подразбиране с Advanced Authentication Framework решение, което поддържа широк спектър от методи за идентификация

■ Централизирано управление на политики (за прилагане на достъп, базиран на роли)

■ Вграден мобилен достъп за потребители на смартфони (iOS и Android), които се нуждаят от достъп до прилежащи приложения

■ Одобрение на достъп, единично вписване и персонализиране чрез вграден Access Gateway

Защо Access Manager

Access Manager дава възможност на организациите да интегрират както съвременни, така и прилежащи уеб базирани приложения. В допълнение към предоставянето на множество опции за Federation, той също така позволява достъп чрез една регистрация до приложения благодарение на своя потребителски графичен интерфейс (GUI), без да е необходимо да променяте приложения или да пишете сложен код.

Access Manager включва вградени функции за определяне на риска, които не изискват сложна конфигурация или настройка, като същевременно предоставят начин да персонализирате идентифицирането на потребителя въз основа на голямо разнообразие от параметри, включително контекст, поведение в миналото, местоположение, време или дори устройство.

Улеснен графичен интерфейс Ви позволява за няколко минути да създадете нов сървър, да направите резервно копие или да мигрирате политиките си от Вашата тестова среда към Вашата работна среда.

Със своята подвижна архитектура и интеграция по подразбиране с Identity Manager и Sentinel™ решенията, Access Manager осигурява цялостно решение за управление на идентичност, достъп и

сигурност за Вашите интранет, облачни и мобилни приложения.
Неговият гъвкав и компактен дизайн и превъзходната му производителност правят Access Manager по-лесен за имплементиране и привеждане в работен режим продукт, като се използва значително по-малко хардуер и се използва опростена конфигурация. Като част от продуктова линия, която защитава, следи и управлява достъпа до Вашите ценни ресурси, Access Manager може да служи като компонент на интегрирана IAM стратегия.

Системни изисквания

Администраторска конзола, Admin Console, Identity Server и Access Gateway Service
- 4 GB RAM
- Dual CPU или Core (3.0 GHz или съпоставим чип)
- твърд диск 100 GB
- SUSE Linux Enterprise Server (SLES) 11 SP4 или
- SLES 12 с 64-битова операционна система на хардуер x86-64 (физически или виртуален)

или
- Red Hat Enterprise Linux (RHEL) 6.7 и 7.1 (64-битов) (физически или виртуален)

или
- Windows Server 2012 R2, 64-битов (физически или виртуален)

Access Gateway Appliance и Access Manager Appliance
- 8 GB RAM
- Dual CPU или Core (3.0 GHz или съпоставим чип)
- твърд диск от 100 GB

Устройството работи с 64-битова операционна система на хардуер x86-64, поддържан от SLES 11 SP4.
За списък на хардуера x86-64 със поддръжка на SLES 11 SP4 и SLES 12, вижте бюлетина за налични сертификати публикуван на: www.suse.com/yessearch/Search.jsp

---

Подписаната, [redacted], *ЕГН:* [redacted] *Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ , извършен от мен. Преводът се състои от 4 страници.*

Подпис: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

MICRO FOCUS

Data Sheet
Security

Access Manager

Micro Focus is a leading provider of web single sign-on solutions that deliver transparent, secure access to applications and services.. Supporting federation standards, NetIQ® Access Manager™ enables organizations to share private information across web, cloud and mobile securely and conveniently. Because granting secure access is more than just knowing who needs it, Access Manager adapts to the right level of user identification based on measured risk to the business.

Product Overview

Access Manager delivers user single sign-on and secure access to intranet and cloud-based applications from wherever the user is located: the office, remote, on the road; or for consumers, from whatever device they are using. Access Manager does this by supporting federation standards for today's modern applications and services while still keeping its best-of-breed gateway capabilities for everything else. In addition to single sign-on and access control, Access Manager includes a built-in, risk-based engine and two-factor authentication, so organizations can keep access simple when risk is low and adapt user verification when risk is high or in between. It's designed to use less hardware, deploy faster, and require less maintenance, giving you faster time to value and lower cost of ownership.

For organizations that don't already have one, Access Manager includes a customizable login page and mini application portal, so organizations can brand them as needed. The application icons are configurable and adapt to the form factor from which they are consumed, all of which requires minimal time and expertise. From beginning to end, Access Manager is designed for simplicity and low cost of ownership.

Key Benefits

Access Manager is the right fit for delivering single sign-on and secure access to web-based applications. With its rich set of features built right into the product and its simplified design and integration with other Micro Focus® identity and access solutions, you can avoid complex and siloed configurations. Access Manager empowers organizations to do more with less, delivering quick and convenient access for users while keeping private information secure. With Access Manager, your organization can:

- Deliver secure access across the organization—Access Manager is a full-featured access solution that delivers single sign-on for modern federated services that support SAML, WS-Federation, WS-Trust, OAuth and OpenID, as well as applications and services without federation support.
- Score quick wins for your mobile strategy—Whether you need single sign-on for your internally developed corporate mobile apps or for your legacy web apps, Access Manager has the solution. It comes with an SDK that enables application federation for developers, as well as a mobile gateway that delivers one-touch access to legacy web apps on mobile form factors in just hours. Either way, you're able to implement identity and access control without touching your back-end applications.

System Requirements

Admin Console, Identity Server and Access Gateway Service

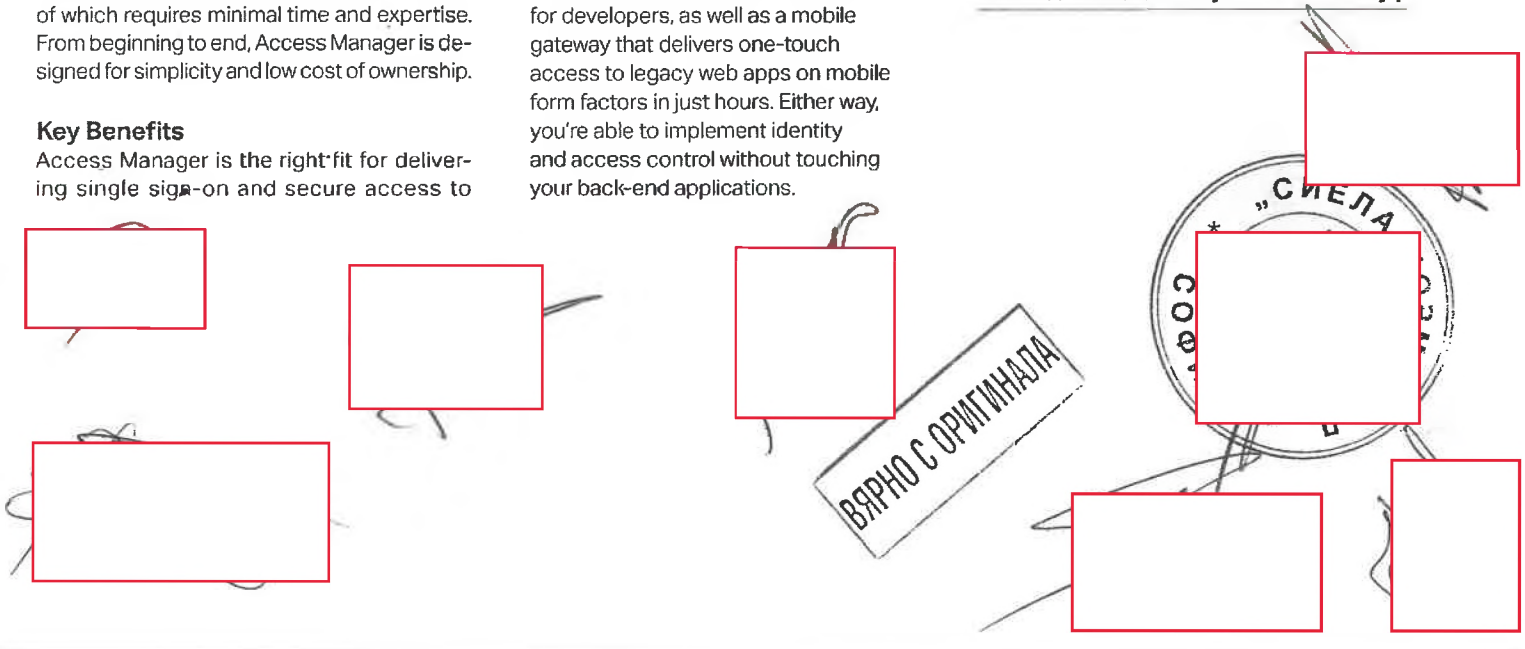
- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk
  - SUSE Linux Enterprise Server (SLES) 11 SP4
    Or
  - SLES 12 with 64-bit operating system x86-64 hardware (physical or virtual)
    Or
  - Red Hat Enterprise Linux (RHEL) 6.7 and 7.1 (64-bit) (physical or virtual)
    Or
  - Windows Server 2012 R2, 64-bit (physical or virtual)

Access Gateway Appliance and Access Manager Appliance

- 8 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

The appliance runs 64bit operating system on x86-64 hardware supported by SLES 11 SP4.

For a list of x86-64 hardware with SLES 11 SP4 and SLES 12 support, see the YES CERTIFIED Bulletin at: **www.suse.com/yessearch/Search.jsp**



...rease security and convenience ...ogether—Access Manager has a built-in, risk-based authentication engine that allows organizations to adapt their user's authentication experience based on measured risk, allowing users frictionless access for low risk environments and a step-up authentication for higher risk situations.

- Integrates with otherMicro Focus identity, access, and security products that equip organizations to deliver convenient access to those who need it while protecting organizations from those who don't, both inside and out

Key Features

Enterprises use Access Manage to integrate access to their applications and services across all of their business units, regardless of who owns the user repositories. Its federation and gateway capabilities allow you to bridge together cloud and Intranet applications into a seamless single sign-on and access experience.

- Full support for federation implementations using SAML, OAuth, OpenID Connect, WS-Federation, and others
- UI designer for login and portal pages allows custom branding and icon configuration
- Optional virtual appliance-ready form factor, which is hypervisor agnostic (deploy in almost any environment)
- Out-of-the-box integration with Microsoft SharePoint and Office 365 Enterprise
- Software development kit for iOS devices
- Built-in, risk-based authentication engine that provides risk scoring and selective authentication based on score
- Out-of-the-box integration with Advanced Authentication Framework that supports a wide range of authentication methods
- Centralized policy engine (for role-based access enforcement)
- Built-in mobile gateway for users on smartphones (iOS and Android) who need access to legacy applications
- Access Authorization, single sign-on, and personalization through built-in Access Gateway

Why Access Manager

Access Manager enables organizations to integrate modern as well as legacy web-based applications. In addition to providing multiple federation options, it also allows single sign-on access for applications through its GUI without the need to modify applications or write complex code.

Access Manager includes a built-in risk engine that's free of complex configuration or setup while providing a way to customize the user's authentication experience based on a wide variety of parameters, including context, historical pattern, location, time, or even device.

The Wizard-based code promotion utility allows you to bring up a new server, make a backup, or migrate your policies from your test environment to your production environment in a matter of minutes.

With its pluggable architecture and default integration with Identity Manager and Sentinel™ security, Access Manager provides comprehensive identity, access and security for your intranet, cloud and mobile applications.

Its flexible and compact design and superior performance make Access Manager easier to get up and running, using notably less hardware and simplified configuration. And as part of a product line that secures, monitors, and governs access to your valued resources, Access Manager can serve as a component of an integrated IAM strategy.

Contact us at:
www.microfocus.com

Like what you read? Share it.

Privileged Account Manager

С Privileged Account Manager Вашата организация може да контролира и следи привилегирования потребителски достъп в бази от данни, приложения и в облака.

Представяне на продукта

Според експерти, половината от всички нарушения на сигурността идват от вътре в организациите. Вътрешните заплахи са особено сериозни, когато се свързват със служители, които имат по-високи права на достъп от необходимите. Независимо дали злоупотребата с привилегии се извършва от самия служител или е работа на киберпрестъпник, който е използвал идентификационните данни за достъп на човек вътре в организацията, за да получи достъп до Вашата ИТ мрежа, можете най-добре да контролирате този риск, като внимателно управлявате и наблюдавате какво привилегированите потребители, като супер потребителите и администраторите на бази от данни, правят със своя достъп.

NetIQ® Privileged Account Manager елиминира необходимостта от разпространение на основни идентификационни данни за акаунтите на целия Ви административен персонал. Той делегира административния достъп чрез централизирани политики. Вие конфигурирате тези правила, за да разрешите или откажете потребителска активност въз основа на цялостен модел „кой, какво, къде, кога“, който изследва името на потребителя, въведената команда, името на хоста и времето. Управлявайки привилегиите по този начин, можете да контролирате кои команди имат право да изпълняват потребителите, по кое време и от какво местоположение.

Privileged Account Manager разполага с Enterprise Credential Vault, криптирано хранилище за пароли, което осигурява сигурно съхранение на паролите за Вашите системи, приложения и база от данни.

Enterprise Credential Vault Ви помага централизирано да управлявате привилегированите акаунти на Вашата организация и предоставя интуитивен интерфейс за привилегированите потребители да проверяват статуса на паролите им. Той също така дава възможност за обширна поддръжка на различни видове привилегировани акаунти, като например за приложения (като SAP система), бази от данни (като Oracle DBMS) и облачни услуги (като Salesforce.com.).

С единствения в индустрията базиран на drag-and-drop графичен потребителски интерфейс, Privileged Account Manager опростява процеса на създаване на правила и на практика премахва необходимостта от сложни скриптове въвеждани на ръка. Интегрираният инструментариум с набор от тестове Ви позволява да моделирате и тествате нови комбинации от правила, преди да ги пуснете в широка употреба.

Използвайки уникален механизъм за анализ на риска, Privileged Account Manager анализира всяка команда, докато тя бъде въведена и ѝ присвоява ниво на риск от 0 до 9 въз основа на изпълнената команда, потребителя, който я е изпълнил и местоположението. Командите с висок риск са кодирани в червен цвят, а командите с нисък риск са кодирани в зелен цвят, с различни нюанси между тях за незабавно идентифициране на събития, които биха могли да представляват риск за сигурността. Освен това можете да видите всяка записана активност на натискане на клавиш чрез интуитивен интерфейс с функции за възпроизвеждане. Ако едно

ЕТ „Л и С - Стилияна Махалджийска“
Офис „Изток“: 1113 София, ул. Жолио Кюри 46Б, тел./факс: 02 963 44 04
Офис „Младост 1“: 1784 София, бул. Йерусалим, бл. 54, офис 11, партер (в двора), тел./факс: 02 974 57 55
Офис „Бизнес парк София“: 1715 София, Бизнес парк София, сграда 8, вх. А- Б, тел.: 02 489 81 55
ET „L&S - Stiliyana Mahaldjiiska“
Office „Istok“: 1113 Sofia Bulgaria, 46B, Fr. J. Curie Str., tel./fax: 02 963 44 04
Office „Mladost 1“: 1784 Sofia Bulgaria, 54, Yerusalim Blvd., Office 11, ground floor, tel./fax: 02.974 57 55
Office „Business Park Sofia“: 1715 Sofia Bulgaria, Business Park Sofia, building 8, ent. A-B, tel.: +359 2 489 81 55
office@variante.info
sliai@abv.bg
+359 888 875 932
www.variante.info

събитие изисква допълнителен анализ, работен процес ескалира събитието до подходящите мениджъри, които могат да предприемат незабавни действия.
Privileged Account Manager разширява този базиран на риска контрол на дейности, за да осигури автоматизирано прилагане на политиката по време на сесии на привилегировани потребители. Ако потребителят извършва рискова дейност, като например достъп до ограничени данни или спиране на услуга, администраторът може да конфигурира Privileged Account Manager да прекъсне автоматично сесията или да блокира потребителя от достъп до всички привилегировани акаунти.

Основни предимства

Контролира и наблюдава неоторизиран и неконтролиран достъп на привилегировани потребители в цялата Ви разнородна среда.
- Управлява централизирано политиките за сигурност от една точка.
- Непрекъснато подкрепя спазването на вътрешните политики и външните разпоредби.
- На практика елиминира нуждата от сложни скриптове въвеждани на ръка.
- Прилага последователна политика във Вашата среда чрез централизирано управление.
- Активира прилагането, анализа и отчитането на достъпа, за да отговаря на законите изисквания и разпоредбите за поверителност.

Основни функции

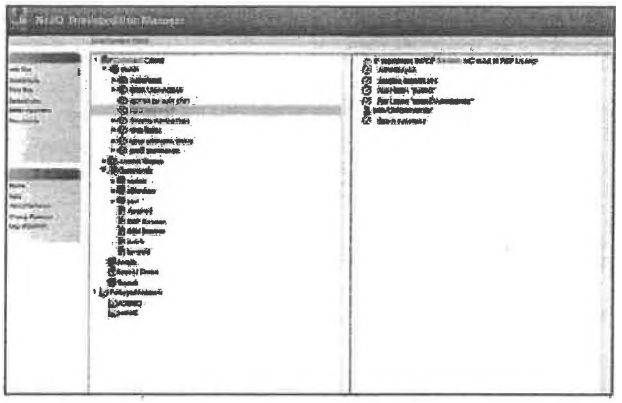
Проектира, конфигурира, тества и внедрява решение за управление на привилегировани акаунти в цялата Ви среда от едно място.
- Enterprise Credential Vault за криптирано съхранение на пароли в хранилище
- Наблюдение на бази от данни за действия от привилегировани акаунти на потребители, инструменти и приложения
- Контрол на сесията, базиран на риска, за да се позволи автоматично прекратяване на сесията или отмяна на достъп
- Дистанционно създаване на сесии и контрол на операционните системи
- Профилиране на риска, което бързо идентифицира потребителите с висок риск
- Интелигентни оценки на риска, изградени на базата на анализ на потенциални заплахи

Ключови отличителни черти

Получавате най-изчерпателната отчетност за събития за спомагане при извършване на одит. С Privileged Account Manager имате възможност да одитирате всички потребителски дейности със 100-процентово регистриране на натискания на клавиши и заснемане на видео за всички базирани на идентифициране среди, включително приложения като SAP система, бази данни като Oracle DBMS и облачни услуги като Salesforce.com.
За конкретни събития за достъп одиторите могат да възпроизвеждат цялото събитие на ниво натискане на клавиша - с цветно кодирани подробности по ред - и да използват статус „разрешен“ или „неоторизиран“ към всяко събитие.
За да научите повече за Privileged Account Manager или да започнете пробен период на тестване, отидете на уеб-страницата на производителя.

Системни изисквания

За подробен списък с платформи, които Privileged Account Manager поддържа, и изисквания за инсталиране, вижте ръководството за инсталиране на портала на Micro Focus.



Фигура 1. Конзолата за управление на командите позволява на администраторите да защитават и контролират потребителски команди.

Подписаната, [redacted] *ЕГН:* [redacted]*, Потвърждение №: 18ПР-1398/26.02.2018 г., удостоверявам верността на превода от английски на български език на приложения документ , извършен от мен. Преводът се състои от 4 страници.*

Подпис: [redacted]

MICRO FOCUS L&S София ЕТ "ПиС - Ст. Махалиски"

[redacted]

MICRO FOCUS

Data Sheet
Security

Privileged Account Manager

With Privileged Account Manager, your organization can control and monitor privileged user access across databases, applications, and the cloud.

Product Overview

Experts estimate that as many as half of all security breaches come from inside organizations. Insider threats are especially serious when associated with employees who have higher access privileges than needed. Whether the privilege misuse occurs at the hands of an employee, or is the work of a cyber-criminal who has leveraged the access credentials of an insider to gain access to your IT network, you can best manage this risk by closely controlling and monitoring what privileged users, such as super-users and database administrators, are doing with their access.

NetIQ® Privileged Account Manager eliminates the need to distribute root-account credentials to your entire administrative staff. It delegates administrative access using centralized policies. You configure these policies to allow or deny user activity based on a comprehensive "who, what, where, when" model that examines the user's name, typed command, host name and time. By managing privileges this way, you can control what commands users are authorized to run, at what time and from what location.

Privileged Account Manager features an Enterprise Credential Vault, or an encrypted password "vault," that provides secure storage of your system, application, and database passwords. The Enterprise Credential Vault helps you to centrally manage your organization's privileged accounts and provides an intuitive interface for privileged users to check-out and return passwords. It also enables broader privilege account support for applications (such as SAP System), databases (such as Oracle DBMS), and cloud services (such as Salesforce.com.)

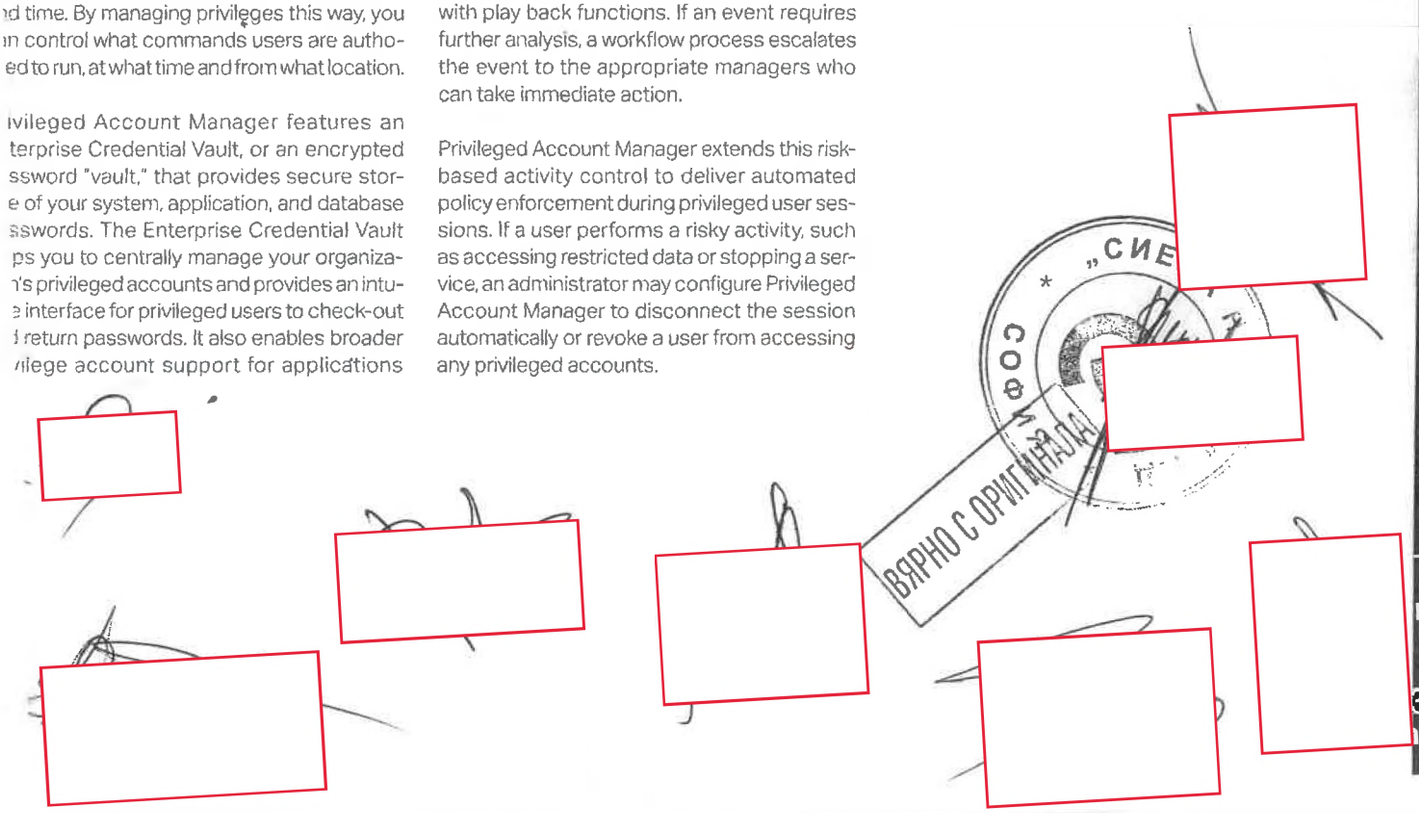
With the industry's only GUI-based, drag-and-drop interface, Privileged Account Manager simplifies the rule-creation process and virtually eliminates the need for complex, manual scripting. An integrated test-suite tool allows you to model and test new rule combinations before committing them to production use.

Using a unique risk-analysis engine, Privileged Account Manager analyzes each command as it is typed and assigns it a risk level from 0 to 9 based on the command executed, the user who executed it, and the location. High-risk commands are color coded as red, and low-risk commands are color coded as green, with varying shades in between for instant identification of events that could pose a security risk. Additionally, you may view any recorded keystroke activity through an intuitive interface with play back functions. If an event requires further analysis, a workflow process escalates the event to the appropriate managers who can take immediate action.

Privileged Account Manager extends this risk-based activity control to deliver automated policy enforcement during privileged user sessions. If a user performs a risky activity, such as accessing restricted data or stopping a service, an administrator may configure Privileged Account Manager to disconnect the session automatically or revoke a user from accessing any privileged accounts.

System Requirements

For a detailed list of platforms that Privileged Account Manager supports, and requirements for installation, please see the Installation Guide here.



Contact us at:
www.microfocus.com

Like what you read? Share it.

Key Benefits

Control and monitor unauthorized and unmonitored privileged user access across your entire heterogeneous environment.

- Centrally manage security policies from a single point.
- Continuously support compliance with internal policies and external regulations.
- Virtually eliminate the need for complex manual scripting.
- Enforce a consistent policy throughout your environment via centralized management.
- Enable access enforcement, analysis and reporting to comply with privacy laws and regulations.

Key Features

Design, configure, test and deploy a privileged account management solution across your entire environment from a single location.

- Enterprise Credential Vault for secured password vaulting
- Database privileged account monitoring for users, tools, and applications
- Risk-based session control to enable automatic session termination or access revocation
- Remote session establishment and control for operating systems
- Risk profiling that quickly identities high-risk users
- Smart risk ratings built on potential threat analysis

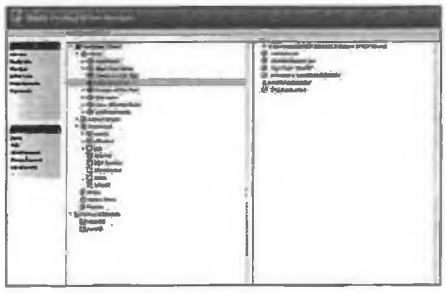


Figure 1. The Command Control Console enables administrators protect and control user commands.

Key Differentiators

Build the most comprehensive audit trail available. With Privileged Account Manager, you have the ability to audit all user activity with 100-percent keystroke logging and video capture for all credential-based environments, including applications such as SAP System, databases such as Oracle DBMS, and cloud services such as Salesforce.com.

For specific access events, auditors may play back the entire event at a keystroke level—with color-coded, line-by-line detail—and apply a status of "authorized" or "unauthorized" to each event.

To learn more about Privileged Account Manager, or to start a trial, go here.

MICRO FOCUS

ПРИЛОЖЕНИЕ № 3.8

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ЦЕНОВО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 8: „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“***
Наименование на участника:	***СИЕЛА НОРМА АД***
Правно-организационна форма на участника:	***Акционерно дружество***
Седалище по регистрация и адрес на управление:	***гр. София, пк 1510, район Подуяне, бул. „Владимир Вазов“ № 9***
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	***ЕИК 130199580***
Представляващ	***Веселин Тодоров Тодоров***

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното ценово предложение по горецитираната обособена позиция:

Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

1. Предлагаме да изпълним доставката, предмет на горецитираната процедура за възлагане на обществена поръчка при следните цени:

№	Описание	Количество	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
I.	II.	III.	IV.	V.
1.	Платформа за управление на идентичността на потребителите	1 брой	**1 364 100.00**	**1 364 100.00**
2.	Система за управление на привилегированите потребители	1 брой	**94 674.00**	**94 674.00**
			Обща цена в лева без ДДС	**1 458 774.00**

2. В цените по т. 1 са включени всички разходи за изпълнение на поръчката. Потвърждаваме, че възложителят няма да дължи заплащането на каквито и да е други разноски, направени от нас като изпълнител.

3. Потвърждаваме, че цените по т. 1 са постоянни за целия срок на договора и не подлежат на промяна за времето на изпълнение на договора, освен в случаите когато това е в полза на възложителя.

Приложения: Количествено-стойностна сметка

Забележка:

1. *Предложените от участника цени следва да са в български лева без ДДС, закръглени до втория знак на десетичната запетая.*

2. *Участник, който допусне аритметична грешка, се отстранява от участие в процедурата по съответната обособена позиция.*

3. *Участник, който предложи обща цена, която е по-висока от прогнозната стойност на съответната обособена позиция, се отстранява от по-нататъшно участие в процедурата по съответната обособена позиция.*

4. *Липсата на ценово предложение, както и предоставянето на ценово предложение, което не отговаря на изискванията на документацията за обществената поръчка, е основание за отстраняване от по-нататъшно участие в процедурата по съответната обособена позиция.*

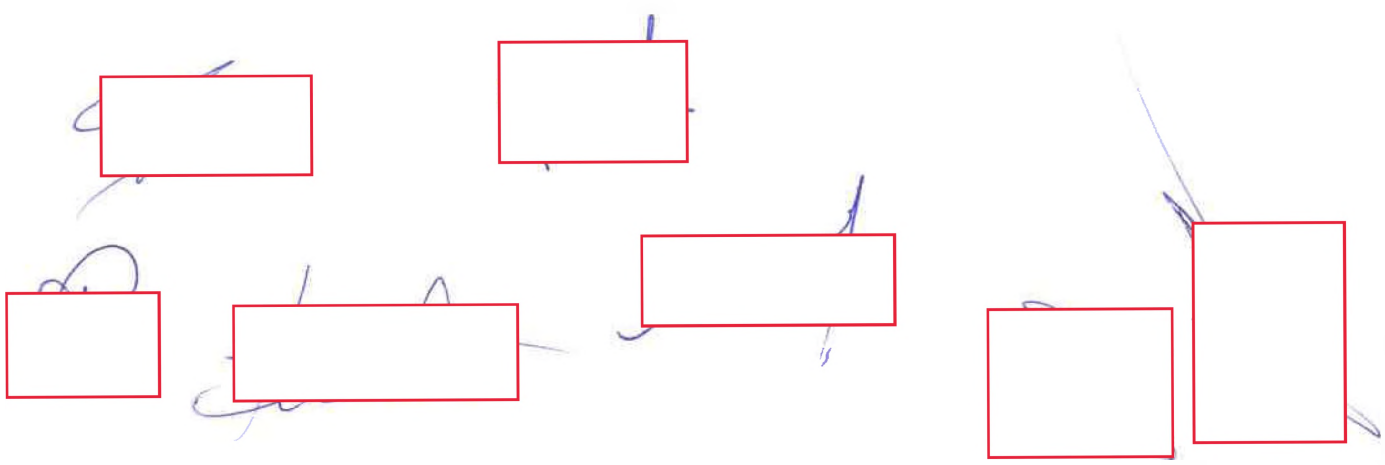
Дата на подписване: 0/07 / 2020 г.

Подпис и печат: .....

Име и фамилия Веселин Тодоров

Длъжност Изпълнителен директор

Наименование на участника Сиела Норма АД



ПРИЛОЖЕНИЕ

към Ценово предложение

от фирма СИЕЛА НОРМА АД

по *Обособена позиция № 8: „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“*

КОЛИЧЕСТВЕНО-СТОЙНОСТНА СМЕТКА

I. Платформа за управление на идентичността на потребителите

№	Продукт	Тип	Продуктов №	Бр.	Ед. цена лв. без ДДС	Обща цена лв. без ДДС
1	Базова система за управление и контрол на цифровите идентичности и достъпа до информация **Micro Focus Identity & Access Management Base License** (per affiliated/enterprise entity)	софтуер	873-011081	1	955.00	955.00
2	Първоначална едногодишна поддръжка на базовата система Identity & Access Management **Initial Business Support** (per affiliated/enterprise entity)	поддръжка	877-008261-I	1	213.00	213.00
3	Едногодишна поддръжка на Identity & Access Management Base **Renewal Business Support** (per affiliated/enterprise entity)	поддръжка	877-008261	1	213.00	213.00
4	Едногодишна поддръжка на Identity & Access Management Base **Renewal Business Support** (per affiliated/enterprise entity)	поддръжка	877-008261	1	213.00	213.00
5	Едногодишна поддръжка на Identity & Access Management Base **Renewal Business Support** (per affiliated/enterprise entity)	поддръжка	877-008261	1	213.00	213.00
6	Едногодишна поддръжка на Identity & Access Management Base **Renewal Business Support** (per affiliated/enterprise entity)	поддръжка	877-008261	1	213.00	213.00

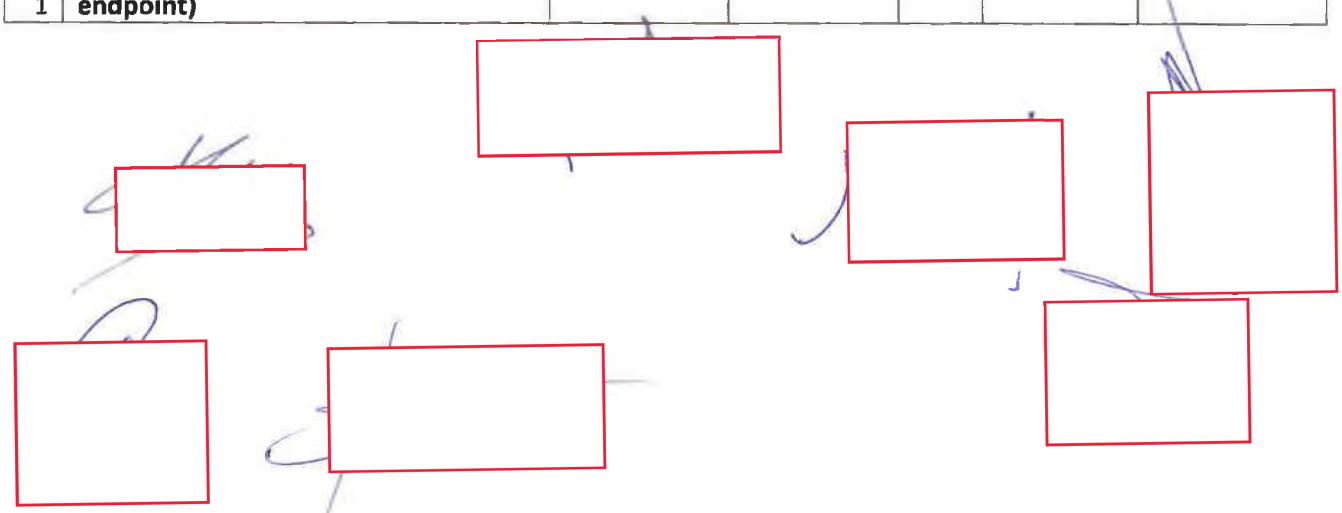
Заличаванията на информация в документа са на основание чл. 4 от Общ регламент за защита на данните

7	Модул за контрол на достъпа до информация **Micro Focus Access Manager License Add-on (per managed identity)**	софтуер	873-011097	8000	16.00	128,000.00
8	Първоначална едногодишна поддръжка на Access Manager Add-on **Initial Business Support** (per managed identity)	поддръжка	877-008293-I	8000	3.45	27,600.00
9	Едногодишна поддръжка на Access Manager Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008293	8000	3.45	27,600.00
10	Едногодишна поддръжка на Access Manager Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008293	8000	3.45	27,600.00
11	Едногодишна поддръжка на Access Manager Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008293	8000	3.45	27,600.00
12	Едногодишна поддръжка на Access Manager Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008293	8000	3.45	27,600.00
13	Модул за управление и контрол на цифровите идентичности **Micro Focus Identity Management Administration License Add-on (per managed identity)**	софтуер	873-011082	8000	40.94	327,520.00
14	Първоначална едногодишна поддръжка на Identity Management Administration Add-on **Initial Business Support** (per managed identity)	поддръжка	877-008263-I	8000	10.44	83,520.00
15	Едногодишна поддръжка на Identity Management Administration Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008263	8000	10.44	83,520.00
16	Едногодишна поддръжка на Identity Management Administration Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008263	8000	10.44	83,520.00
17	Едногодишна поддръжка на Identity Management Administration Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008263	8000	10.44	83,520.00

18	Едногодишна поддръжка на Identity Management Administration Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008263	8000	10.44	83,520.00
19	Модул за защитено вписване на потребителите в системите **Micro Focus Secure Login License Add-on (per managed identity)**	софтуер	873-011099	8000	20.87	166,960.00
20	Първоначална едногодишна поддръжка на SecureLogin Add-on **Initial Business Support** (per managed identity)	поддръжка	877-008297-I	8000	4.60	36,800.00
21	Едногодишна поддръжка на SecureLogin Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008297	8000	4.60	36,800.00
22	Едногодишна поддръжка на SecureLogin Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008297	8000	4.60	36,800.00
23	Едногодишна поддръжка на SecureLogin Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008297	8000	4.60	36,800.00
24	Едногодишна поддръжка на SecureLogin Add-on **Renewal Business Support** (per managed identity)	поддръжка	877-008297	8000	4.60	36,800.00
					Обща цена в лв. без ДДС:	**1,364,100.00**

II. Система за управление на привилегированите потребители

№	Продукт	Тип	Продуктов №	Бр.	Ед. цена лв. без ДДС	Обща цена лв. без ДДС
1	Система за управление на привилегированите потребители **Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices (per managed endpoint)**	софтуер	873-011105	300	147.23	44,169.00



2	Първоначална едногодишна поддръжка на Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices **Initial Business Support** (per managed endpoint)	поддръжка	877-008309-I	300	33.67	10,101.00
3	Едногодишна поддръжка на Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices **Renewal Business Support** (per managed endpoint)	поддръжка	877-008309	300	33.67	10,101.00
4	Едногодишна поддръжка на Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices **Renewal Business Support** (per managed endpoint)	поддръжка	877-008309	300	33.67	10,101.00
5	Едногодишна поддръжка на Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices **Renewal Business Support** (per managed endpoint)	поддръжка	877-008309	300	33.67	10,101.00
6	Едногодишна поддръжка на Privileged Account Manager License Add-on for Servers, Applications, or non end-user devices **Renewal Business Support** (per managed endpoint)	поддръжка	877-008309	300	33.67	10,101.00
					Обща цена в лв. без ДДС:	**94,674.00**

Дата: 10.07.2020 г.

Подпис и печат.....

Веселин Тодоров, Изпълнителен директор