### Контактни данни за получаване на сигнал

Получател:

Иван Демерджиев

Email адрес:

[minister@mvr.bg](mailto:minister@mvr.bg)

GPG Fingerprint:

3DAF 842A DAAF 190D AB13 D701 DCCE B6EA 2697 15E7

### Обща информация

Ако искате да се свържете с нас по имейл, но се притеснявате, че съдържанието му би могло да бъде прочетено от някой друг, криптирането с публичен ключ значително ще повиши сигурността. Чрез инсталиране на специализиран за целта софтуер Вие имате възможност да:

* криптирате и декриптирате имейли във Вашия имейл клиент;
* управлявате ключовете на Вашите контакти;
* предпазите съдържанието на Вашите имейли от всички, освен от получателя (дори Вашия имейл доставчик не може да ги прочете).

Криптирането с публичен ключ на имейл съобщения е метод за гарантиране на конфиденциалността на комуникацията. Този метод цели да подсигури това, че само адресанта и адресата имат достъп до съответното съдържание, като елиминира възможността на трети лица без оторизиран достъп да прихванат съобщението.

Криптираният имейл също така не би могъл да бъде прочетен нито от доставчиците (администраторите) на съответните услуги по предоставяне на електронни пощи (домейни), нито от доставчиците на интернет услуги. Той би могъл да бъде прочетен само от хората, за които е предназначен.

Криптирането се осъществява чрез т.нар. “публичен ключ”. Както и името му подсказва, той е общодостъпен и може да бъде използван от всеки. Това е определена последователност от символи - код, който позволява дадено съдържание да бъде криптирано и предназначено за конкретен получател. Публичният ключ може да се разглежда като допълнителен идентификатор, който строго и формално определя лицето, което единствено ще има достъп до криптираното съобщение. Може да се направи аналогия с единния граждански номер (ЕГН) на българските граждани, който еднозначно определя кое е лицето с даден такъв номер.

Веднъж криптирано със съответния публичен ключ, съобщението вече ще е достъпно само за получателя, за който то е предназначено. Получателят достъпва съдържанието чрез неговия “частен ключ”. Частният ключ е друг код, но за разлика от публичния, той е секретен и никой няма достъп до него, с изключение на неговия притежател. Чрез него адресатът дешифрира съобщението, което е било криптирано и предназначено за него.

По този начин, дори криптираното съдържание да попадне в трети лица, то не би могло да бъде “отключено” и достъпено, тъй като това е невъзможно да бъде извършено без частния ключ, който е известен само на получателя. Въпреки че публичния и частния ключ на лицето са свързани, практически е невъзможно от публичния ключ да се достигне до частния благодарение на криптографските алгоритми, които служат за тяхното генериране.

За да можете да получавате криптирани email съобщения в отговор на Вашия сигнал, Вие също ще трябва да си направите двойка ключове - публичен и частен. Първият ще споделите с нас, за да криптираме съдържанието, което е предназначено за Вас, а вторият няма да споделяте с никого. Чрез него Вие ще сте единственият, който ще може да дешифрира изпратеното до Вас съобщение.

Последвайте този {линк}, за да се запознаете с конкретните стъпки необходими за осъществяване на криптирана email комуникация.

### Инструкция за инсталиране и използване на специализирано приложение **Mailvelope.**

##### 1. Инсталирайте Mailvelope във Вашия браузър

Добавете Mailvelope към браузъра си, като използвате една от тези връзки за изтегляне:

* [Mailvelope for Google Chrome](https://chrome.google.com/webstore/detail/mailvelope/kajibbejlbohfaggdiogboambcijhkke?hl=en)
* [Mailvelope for Mozilla Firefox](https://addons.mozilla.org/en/firefox/addon/mailvelope/)
* [Mailvelope for Microsoft Edge](https://microsoftedge.microsoft.com/addons/detail/mailvelope/dgcbddhdhjppfdfjpciagmmibadmoapc)

За да функционира добре, Mailvelope трябва да бъде дълбоко интегриран във Вашия браузър. Ще трябва да дадете на Mailvelope някои разрешения, за да може да добавя нови опции към входящата Ви пощенска кутия. Тези разрешения изглеждат по различен начин във всеки браузър. Mailvelope не чете Вашия имейл или Вашите данни и използва тези разрешения, единствено за да може да интегрира неговите функции във Вашата електронна поща.

##### 2. Отворете Mailvelope

Иконата Mailvelope се намира в горния десен ъгъл на Вашия браузър. Кликнете върху нея, за да настроите Вашите ключове за криптиране.

##### 3. Добавете Вашата двойка ключове

За да изпращате и получавате криптирани съобщения, първо се нуждаете от “двойка ключове“. Екранът за настройка на Mailvelope ще Ви помогне да генерирате нова или да импортирате съществуваща двойка.

|  |
| --- |
|  |

##### 3.1 Ако нямате двойка ключове, може да я генерирате по следния начин

Изберете "Generate key" на екрана за настройка. След това въведете Вашето име (или псевдоним) и имейл адреса, с който искате да бъде свързан новият ви ключ. Изберете сигурна парола, която не използвате за други акаунти. Запишете я на хартия или я запазете в специализирано приложение за мениджмънт на пароли.

*\*Забележка: Тъй като Mailvelope не съхранява Вашата парола, същата не може да бъде възстановена, ако я загубите!*

|  |
| --- |
|  |

Mailvelope ще потвърди успешното създаване на ключ и ще Ви покаже новия ключ на екрана "Key Management".

|  |
| --- |
|  |

За да потвърдите своя ключ и за да сте сигурни, че Вашите партньори в комуникацията ще го намерят, проверете имейлите си и щракнете върху връзката в имейла за потвърждение "Verify your email address" от „Mailvelope Key Server“.

##### 3.2 Ако имате двойка ключове, можете да ги импортирате

Отворете опциите на Mailvelope (запомнете: иконата на Mailvelope се намира в горната дясна част на Вашия браузър) и изберете "Key Management". За да импортирате Вашата двойка ключове, ще Ви трябва файлът (обикновено завършващ на ".asc") и неговата парола. Можете да го импортирате, като плъзнете и пуснете файла в прозореца на браузъра или като го намерите на Вашия компютър с помощта на "Add file".

|  |
| --- |
|  |

След като прикачите файла, кликнете върху бутона “Import keys”. Mailvelope ще Ви покаже някои технически детайли относно ключа, който искате да добавите (Key ID / Fingerprint). След като потвърдите, Вашият ключ ще се появи във Вашия “ключодържател” и вече ще може да се използва.

|  |
| --- |
|  |

За да сте сигурни, че новата двойка ключове е автоматично достъпна за други потребители на Mailvelope, които биха искали да Ви напишат криптиран имейл, може да я качите на сървъра за ключове на Mailvelope (Тези, които не използват Mailvelope, също ще могат да Ви изпращат имейл. За да направите това, щракнете върху вашата двойка ключове. Ще видите оцветено в червено известие, което указва, че „Потребителският идентификатор не е синхронизиран със сървъра за ключове на Mailvelope“. Натиснете бутона "Синхронизиране", за да качите публичния ключ. След това, проверете пощенската си кутия и я верифицирайте като щракнете върху линка в имейла за потвърждение, върху който е изписано „Verify your email address“ от „Mailvelope Key Server“.

##### 4. Добавете ключовете на Вашите контакти

След като вече имате своята двойка ключове, може да добавите и ключовете на Вашите контакти. Ако те също използват Mailvelope вероятно няма да имате много за настройване. Mailvelope Key сървърът ще намери техните публични ключове автоматично.

Просто започнете да пишете на някой от тях имейл съгласно инструкциите в [точка 5](#_bgtduxn4tpnz). Ако след като го вмъкнете, имейлът на получателя от червен стане зелен, това ще означава, че Mailvelope вече е намерил неговия публичен ключ. Ако това обаче не се случи, ще трябва ръчно да добавите неговият ключ към Вашия ключодържател преди да му изпратите криптирано email съобщение. Има два начина да направите това.

##### **4.1**. **Импортиране на файл**

Ако лицето, с което комуникирате Ви изпрати неговия публичен ключ във вид на файл, Вие може да го добавите към ключодържателя си чрез избор на "Key Management" → "Import". Там може да го импортирате чрез “приплъзване” с мишката към прозореца на браузъра или пък да посочите неговото местонахождение на Вашия компютър чрез бутона "Add file".

|  |
| --- |
|  |

##### 4.2. Търсене в директории с ключове

Key сървърите са директории, в които се съхраняват списъци с публични ключове и свързаните с тях email адреси. В тях може да потърсите и публичните ключове на лицата от Вашите контакти.

За целта, изберете "Key Management" → "Search" и въведете email адреса на получателя, до който желаете да изпратите криптирано съобщение. Вградената в приложението функция ще претърси key сървърът на Mailvelope, както и още няколко от най-използваните key сървъри. Ако желаете, Вие също може да редактирате списъка с key сървъри, които да бъдат претърсени.

|  |
| --- |
|  |

##### 5. Криптиране и декриптиране на email през Вашата електронна поща.

С Mailvelope Вие можете да криптирате и декриптирате email съобщения в много уеб-mail платформи. Основните сред тях са описани по-долу.

##### 5.1. Gmail

##### 5.1.1. Изпращане на криптирано съобщение с Gmail

След като Mailvelope е инсталиран на Вашия браузър, Вие ще виждате бутон с логото на Mailvelope непосредствено до бутонът “Compose” (това е бутонът за създаване на ново писмо) на Gmail. Натиснете върху Mailvelope бутона, за да отворите неговия редактор.

|  |
| --- |
|  |

Ако това е първият път, в който използвате Mailvelope за Gmail, ще е необходимо да потвърдите сигнала за сигурност на Google, озаглавен „Използване на API на Gmail“. Ще трябва отново да се впишете във Вашия Google акаунт и да предоставите на Mailvelope достъп до вашия акаунт в Gmail, за да направите възможна дълбоката интеграция на процесите на криптиране/декриптиране.

*\*Забележка: Ако използвате Gmail като част от Google Workspace, може да се наложи да започнете с безплатния тестов период на Mailvelope Business.*

Обратно в редактора на Mailvelope, въведете имейл адреса на получателя в полето за получател. Ако Вашият получател е качил своя ключ на key сървъра на Mailvelope, Mailvelope ще го намери автоматично и имейл адресът ще стане зелен. Ако адресът остане червен, това означава, че Mailvelope не може да намери неговия ключ в сървъра. Можете да импортирате ключа във Вашия ключодържател, като следвате инструкциите в стъпка [4. Добавете ключовете на Вашите контакти](#_ers1hmo7me9z).

|  |
| --- |
|  |

След като добавите публичния ключ на получателя, Вие ще можете да пишете email съобщения и да прикачвате файлове както обикновено, след което да ги изпращате. Цялото съобщение, включително и прикачените файлове, ще бъдат криптирани и недостъпни за никой, освен за получателя.

*\*Забележка: Не описвайте конфиденциална информация в темата (the “Subject” line) на писмото. Mailvelope криптира само съдържанието на писмото и прикачените към него файлове.*

##### 5.1.2. Декриптиране на изпратено до Вас съобщение

Ако изберете криптиран email във Вашата входяща поща, Mailvelope ще Ви го покаже като запечатано писмо. При кликване върху него ще се отвори екран за въвеждане на парола. Въвеждането на паролата, прикачена към Вашия ключ, ще дешифрира и ще отвори съобщението.

|  |
| --- |
|  |

Може да забележите, че Mailvelope е добавил червена стрелка, с натискането на която Вие ще подготвите Вашия отговор също във вид на криптирано съобщение. Щракването върху него ще отвори редактора на Mailvelope, готов за неговото въвеждане.

##### 5.2. Outlook

Когато сте във входящата си кутия в Outlook.com, щракнете върху „Ново съобщение“, за да отворите редактора на Outlook.com. Там ще видите иконата Mailvelope в горния десен ъгъл на полето за писане. Щраквайки върху него, ще отворите редактора на Mailvelope, чрез който ще можете да напишете криптирано съобщение.

|  |
| --- |
|  |

|  |
| --- |
|  |

След това въведете email адреса на получателя в полето. Mailvelope ще намери ключа автоматично (той ще стане зелен), ако Вашият адресат е качил своя ключ на key сървъра на Mailvelope, както Вие най-вероятно сте направили в [стъпка 3. Добавете вашата двойка ключове](#_iep6wl3mh6me).

В случай, че въведеният адрес остане червен, то е възможно получателят да не е потвърдил своята двойка ключове.

*\*Забележка: В този случай Вие можете да добавите техните ключове ръчно, като следвате инструкциите в стъпка* [*4. Добавете ключове на Вашите контакти*](#_ers1hmo7me9z)*.*

Въведете Вашето съобщение. След като щракнете върху „Encrypt“, трябва да въведете паролата, прикачена към Вашия ключ, за да подпишете съобщението си.

|  |
| --- |
|  |

Ще видите, че Mailvelope е криптирал Вашето съобщение и то е прехвърлено към обикновения редактор на Outlook.com.

|  |
| --- |
|  |

Сега може да добавите тема (subject) на писмото (*Забележка*: Темата **не** се криптира от Mailvelope!) и да въведете отново имейл адреса на Вашия получател в полето „До“. С щракване върху бутона „Изпращане“ съобщението се изпраща от Outlook.com.

##### 5.2.1 Дешифриране на имейл, изпратен до Вас

Ако кликнете върху криптиран имейл във входящата си кутия, Mailvelope ще го покаже като запечатано писмо. При кликване върху този символ (запечатания плик), Mailvelope ще поиска паролата, прикрепена към Вашия ключ.

След попълване на паролата ще можете да прочетете криптираното съобщение.