Beveiliging

‘Local box’

Document Door Leendert Versluijs

Versie 0.5

Datum 13-05-2014

Contact Toine Veenhuis

Senior-Projectmanager



Belastingdienst / Centrum voor Applicatieontwikkeling en -onderhoud

John F. Kennedylaan 8 | 7314 PS | Apeldoorn

M 06 1860 8468

T 055 528 1963

E [jla.veenhuis@belastingdienst.nl](mailto:jla.veenhuis@belastingdienst.nl)

Inhoud

[0 Beveiliging van LocalBox 4](#_Toc388962124)

[0.1 Uitgangspunten bij ontwikkeling van de app 4](#_Toc388962125)

[0.2 Belangrijkste risico’s 5](#_Toc388962126)

[0.3 Beperkingen vanuit UX 5](#_Toc388962127)

[0.4 Recovery 5](#_Toc388962128)

[0.5 Beveiliging in hoofdlijnen 5](#_Toc388962129)

[1 De app configuratatie 6](#_Toc388962130)

[1.1.1 Werkwijze in de app 6](#_Toc388962131)

[2 Functionaliteit 7](#_Toc388962132)

[2.1 Nieuwe gebruiker logt voor eerste keer aan 7](#_Toc388962133)

[2.2 Toevoegen van een bestand in onbeveiligde hoofdfolder 7](#_Toc388962134)

[2.3 Toevoegen van een bestand in beveiligde hoofdfolder 7](#_Toc388962135)

[2.4 Nieuwe onbeveiligde hoofdfolder 7](#_Toc388962136)

[2.5 Nieuwe beveiligde hoofdfolder 8](#_Toc388962137)

[2.6 Downloaden van een bestand uit een beveiligde folder 8](#_Toc388962138)

[2.7 Delen van een onbeveiligde hoofdfolder 8](#_Toc388962139)

[2.8 Delen van een beveiligde hoofdfolder 8](#_Toc388962140)

[2.9 Delen verwijderen op een beveiligde hoofdfolder 9](#_Toc388962141)

[2.10 Delen van een bestand in een onbeveiligde hoofdfolder met onbekende gebruikers 9](#_Toc388962142)

[2.11 Verwijderen bestand/niet hoofdfolder 9](#_Toc388962143)

[2.12 Verwijderen hoofdfolder 9](#_Toc388962144)

[2.13 Verplaatsen bestand naar andere hoofdfolder of subfolder daarvan 10](#_Toc388962145)

[2.14 Updaten van een bestand 10](#_Toc388962146)

[3 Bestaande API Overzicht 10](#_Toc388962147)

Versiehistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Auteur | Datum | Omschrijving |
| 0.1 | Leendert Versluijs | 15-04-2014 | Eerste opzet (in de mail) |
| 0.2 | Leendert Versluijs | 25-04-2014 | Bijgewerkt |
| 0.3 | Leendert Versluijs | 29-04-2014 | Uitwerking encryptie toevoeging |
| 0.4 | Leejanne Hollaar | 08-05-2014 | Styling document |
| 0.5 | Leejanne Hollaar | 13-05-2014 | Versleutelde en onversleutelde mappen |
|  |  |  |  |

# Beveiliging van LocalBox

## Uitgangspunten bij ontwikkeling van de app

Er wordt uitgegaan van de volgende uitgangspunten

* Per hoofdfolder kan aangegeven worden of deze en alle onderliggende folders en bestanden versleuteld moeten zijn.
* Nieuwe hoofdfolders die in de app aangemaakt worden zijn standaard versleuteld.
* Nieuwe hoofdfolders die op de web interface worden aangemaakt zijn niet versleuteld.
* Nieuwe hoofdfolders die op de win7 sync client aangemaakt worden zijn standaard versleuteld.
* In de web interface zijn versleutelde hoofdfolders niet toegangelijk.
* App en win7 sync client ondersteunen ook onversleutelde hoofdfolders.

Alle volgende uitgangspunten gelden voor beveiligde hoofdfolders en bestanden in beveiligde hoofdfolders. De onbeveiligde folders zijn buiten beschouwing gelaten aangezien het gaat om de beveiliging aspecten duidelijk te krijgen.

* Bestanden worden op een PGP achtige wijze uitgewisseld waarbij voor de encryptie van bestanden AES(256) wordt gebruikt en voor encryptie van de bestands-versleutelings-keys RSA(2048)
* Bestanden staan versleuteld op de server mits de hoofd folder gemarkeerd is voor encryptie;
* Bestanden staan versleuteld op een device;
* Bestanden staan onversleuteld op een filesystem met sync optie (win7 sync client);
* Alle bestanden in een folder en alle subfolders worden met dezelfde AES256 key versleuteld. Let op: key = key + IV.
* De AES256 key + IV zelf staat versleuteld op de server;
* Delen van een folder kan alleen voor hoofd-folders direct in de root, subfolders en bestanden daarin worden automatisch ook gedeeld;
* Delen van een folder is altijd op niveau van een gebruiker, er is geen ondersteuning voor groepen;
* AES256 key per gebruiker (eigenaar + iedereen waarmee de folder is gedeeld) een versleutelde AES256 bestand op basis van public key;
* De private RSA2048 key wordt versleuteld met AES256 op basis van een langere pass-phrase;
* De public RSA2048 keys zijn readonly beschikbaar voor iedereen;
* Om bestanden onversleuteld te delen met onbekenden worden deze bestanden versleuteld opgeslagen en kunnen via een url met daarin de key onversleuteld worden opgevraagd.
* Bestanden kunnen via de web interface onversleuteld gedownload worden na het ingeven van pass-phrase van de eigen private key, de server kan dan het bestand onversleuteld aanbieden; [NOG NIET ONDERSTEUND]
* Folders kunnen via de web interface gedeeld worden na het ingeven van pass-phrase van de eigen private key, de server kan dan een AES256 key bestand aanmaken dat is versleuteld met de eigen private key; [NOG NIET ONDERSTEUND]
* Sleutels worden op het device in de versleutelde database opgeslagen;
* Pass-phrase en access token worden op het device in de versleutelde database opgeslagen;
* De device database versleuteling is op basis van een pincode + uniek id device;
* De sync module slaat op de computer de pass-phrase en access token op;
* Tijdens de sync actie worden bestanden versleuteld of ontsleuteld op een computer;
* Webpagina’s waar om een password of pass-phrase wordt gevraagd zijn altijd https (SSL) [NOG NIET ONDERSTEUND]
* Hoofdfolders kunnen niet verplaatst of gekopieerd worden.

## Belangrijkste risico’s

* Opslag van pass-phrase voor private key op computer voor sync.

## Beperkingen vanuit UX

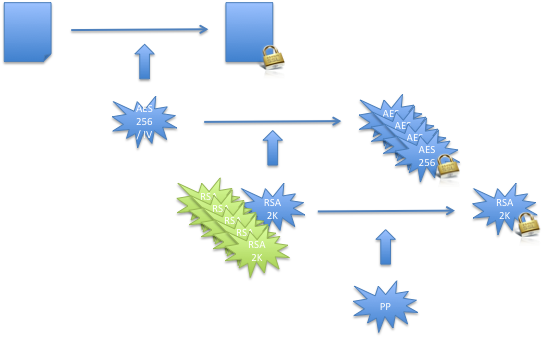
* Bij meeste acties hebben een pass-phrase nodig van gebruiker in de web interface, dit is vervelend voor gebruikers die primair de web interface gebruiken. [NOG NIET ONDERSTEUND]
* Voorlopig nog geen toegang tot beveiligde folders

## Recovery

* password reset door server
* pass-phrase kan in sync en device uitgevraagd worden. [NOG NIET ONDERSTEUND]

## Beveiliging in hoofdlijnen

* Device: alle keys in database en toegang tot database middels pincode die niet op device staat. bestanden staan versleuteld op device. Alleen tijdens “Openen in andere app” tijdelijk onversleuteld.
* Sync: uitgangspunt is dat device beveiligd is. Bestanden staan onversleuteld op disk en pass-phrase staan op computer en is daarmee te achterhalen. Pass-phrase zonder password is niet zinvol zonder toegang tot server.
* Web: uitgangspunt is dat je altijd de pass-phrase moet ingeven om bestanden te ontsleutelen en altijd moet inloggen met password voordat je toegang hebt. Password wordt nergens opgeslagen omdat we met OAuth authenticeren voor Sync en App. [NOG NIET ONDERSTEUND]
* Server: bestanden versleuteld (AES256), key voor bestand ook versleuteld (RSA2048), private key voor versleutelde key voor bestand ook versleuteld (AES256), pass-phrase voor ontsleutelen staat niet op server.



# De app configuratatie

<a

href="lbox://localbox.letshare.com/[usernamekey encoded].json">Registreer in App</a>

[usernamekey encoded].json voorbeeld:

{

“BaseUrl” : “https://localbox.letshare.com/“,

“Name” : “Letshare LocalBox”,

“User” : “account”,

“LogoUrl” : "https://localbox.letshare.com/logo.jpg”,

“BackColor” : “0x808080”,

“TextColor” : “0x000000”,

“APIKey”: “133252352352325”,

“APISecret”:”22352262525235235235235” [MOET NOG ARRAY WORDEN]

}

Bestand is dynamisch zodat de account naam er ook in kan.

### Werkwijze in de app

Gebruiker opent app.

Gebruiker wil localbox toevoegen.

Instructie en openen in-app browser.

Gebruiker typt url in.

Gebruiker logt in.

Kiest de registratie link (lbox://localbox.letshare.com/[usernamekey encoded].json )

LocalBox app download localbox.letshare.com/[usernamekey encoded].json via http of https afhankelijk van server.

Instelling worden opgeslagen en localbox instance wordt geregistreerd.

Invoeren app pincode (eerste box), wachtwoord, pass phrase.

# Functionaliteit

## Nieuwe gebruiker logt voor eerste keer aan

|  |  |
| --- | --- |
| Device | Aanmaken RSA2048 keys op device  Opslaan keys in database  Invoeren pass-phrase en opslaan in database  Private key versleutelen met AES256 op basis pass-phrase  Op de server de keypair registreren via api  Onversleutelde map Publiek aanmaken |
| Sync | Aanmaken RSA2048 keys op computer  Invoeren pass-phrase en opslaan op computer  Private key versleutelen met AES256 op basis pass-phrase  Op de server de keypair registreren via api |
| Web | [NIET ONDERSTEUND]  Aanmaken RSA2048 keys op server  Invoeren pass-phrase  Private key versleutelen met AES256 op basis pass-phrase  Keypair opslaan bij user |

## Toevoegen van een bestand in onbeveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | Gebruiker kiest voor een bestand 'Openen in LocalBox’  LocalBox accepteert het bestand en laat de gebruiker een folder kiezen of een nieuwe folder aanmaken  Het bestand wordt opgeslagen  Bestand wordt geupload naar server |
| Sync | Gebruiker kopieert een bestand naar een LocalBox folder  Bestand bij sync actie uploaden |
| Web | Gebruiker upload bestand |

## Toevoegen van een bestand in beveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | Gebruiker kiest voor een bestand 'Openen in LocalBox’  LocalBox accepteert het bestand en laat de gebruiker een folder kiezen of een nieuwe folder aanmaken  In het geval van een nieuwe hoofd-folder wordt er een nieuwe AES256 key gegenereerd en in de database opgeslagen  Het bestand wordt met de key van folder versleuteld en opgeslagen  Key wordt geregistreerd op server  Bestand wordt geupload naar server |
| Sync | Gebruiker kopieert een bestand naar een LocalBox folder  Bestand wordt bij sync actie versleuteld met de key voor de folder alvorens te uploaden |
| Web | [NIET ONDERSTEUND]  *Gebruiker wordt gevraagd om pass phrase*  *Gebruiker upload bestand*  *Private key wordt uitgepakt met pass phrase*  *Key voor de folder wordt uitgepakt met de private key*  *Bestand wordt versleuteld met key voor de folder* |

## Nieuwe onbeveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | Niet mogelijk |
| Sync | Niet mogelijk |
| Web | De gebruik geeft de naam van de folder in.  Folder wordt aangemaakt op de server |

## Nieuwe beveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | De gebruik geeft de naam van de folder in.  Er wordt een nieuwe AES256 key gegegenereerd en in de database opgeslagen  De key wordt versleuteld met de private RSA key voor de eigen public key  Folder wordt aangemaakt op de server  Versleutelde key wordt geregistreerd op de server |
| Sync | Er is een nieuwe root folder aangemaakt door de gebruiker.  Er wordt een nieuwe AES256 key gegegenereerd  De key wordt versleuteld met de private RSA key voor de eigen public key  Folder wordt aangemaakt op de server  Versleutelde key wordt geregistreerd op de server |
| Web | [NIET ONDERSTEUND]  *De gebruiker geeft de naam van de folder in.*  *De gebruiker moet de pass-phrase invoeren.*  *Er wordt een nieuwe AES256 key gegegenereerd*  *Private key wordt uitgepakt met pass phrase*  *De key wordt versleuteld met de private RSA key voor de eigen public key*  *Folder wordt aangemaakt op de server*  *Versleutelde key wordt geregistreerd* |

## Downloaden van een bestand uit een beveiligde folder

|  |  |
| --- | --- |
| Device | De gebruik kiest een bestand.  Het versleutelde bestand wordt gedownload naar het device.  Als de sleutel van de folder wordt indien nodig van de server gehaald.  Indien de sleutel op gehaald moet worden wordt de private key gebruikt om het key bestand te ontsleutelen.  Bestand wordt tijdelijk onversleuteld op ‘disk’ gezet zodat het bekeken kan worden.  Bestand wordt verwijderd na bepaalde periode of bij sluiten van de app. |
| Sync | Bestand is nieuw op de server en moet opgehaald worden in sync.  Bestand wordt gedownload  Private key opgehaald en ontsleuteld op basis pass phrase (private key kan in memory gecached worden)  Key van bestand opgehaald en ontsleuteld met private key  Bestand ontsleuteld en in folder geplaatst |
| Web | [NIET ONDERSTEUND]  *De gebruiker selecteert downloaden van een bestand.*  *De gebruiker geeft de pass phrase.*  *Private key wordt ontsleuteld met pass phrase.*  *Folder key wordt ontsleuteld met private key.*  *Bestand wordt ontsleuteld met folder key en gestreamed naar de client.* |

## Delen van een onbeveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker zoeken.  API aanroep om folder te delen |
| Sync | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker zoeken.  API aanroep om folder te delen |
| Web | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker zoeken.  Folder delen geregistreerd |

## Delen van een beveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker zoeken.  Gebuiker public key ophalen.  AES256 key/IV versleutelen met eigen private key en public key gebruiker.  Versleutelde key registreren. |
| Sync | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker zoeken.  Gebruiker public key ophalen.  AES256 key/IV versleutelen met eigen private key en public key gebruiker.  Versleutelde key registreren. |
| Web | [NIET ONDERSTEUND]  *Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).*  *Gebruiker zoeken.*  *Gebruiker public key ophalen.*  *AES256 key/IV versleutelen met eigen private key en public key gebruiker.*  *Versleutelde key opslaan.* |

## Delen verwijderen op een beveiligde hoofdfolder

|  |  |
| --- | --- |
| Device | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker kiezen.  Share registratie verwijderen via api.  Key verwijderen voor gebruiker/path combi via api. |
| Sync | Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker kiezen.  Share registratie verwijderen via api.  Key verwijderen voor gebruiker/path combi via api. |
| Web | [NIET ONDERSTEUND]  Lijst bestaande gebruikers met wie gedeeld is wordt opgehaald (meta).  Gebruiker kiezen.  Share registratie verwijderen.  Key verwijderen voor gebruiker/path combi. |

## Delen van een bestand in een onbeveiligde hoofdfolder met onbekende gebruikers

|  |  |
| --- | --- |
| Device | Selecteren bestand en extern delen kiezen.  API aanroepen om de url te verkijgen  Email openen met url erin. |
| Sync | Selecteren bestand en extern delen kiezen.  API aanroepen om de url te verkijgen  Email openen met url erin |
| Web | ? |

## Verwijderen bestand/niet hoofdfolder

|  |  |
| --- | --- |
| Device | Kies een bestand.  Roep de API aan om het bestand te verwijderen.  In het geval van een folder worden alle onderliggende folders en bestanden verwijderd. |
| Sync | Bestand is verwijderd op filesystem.  In sync stap wordt bestand via API verwijderd.  In het geval van een folder worden alle onderliggende folders en bestanden verwijderd. |
| Web | [NIET ONDERSTEUND]  Gebruiker kiest verwijderen bestand.  Bestand wordt verwijderd.  In het geval van een folder worden alle onderliggende folders en bestanden verwijderd. |

## Verwijderen hoofdfolder

|  |  |
| --- | --- |
| Device | Kies een hoofdfolder.  Roep de API aan om de folder te verwijderen.  Alle onderliggende folders, keys en bestanden verwijderd. |
| Sync | Gebruiker verwijdert een hoofdfolder.  Bij de sync actie wordt de API aangeroepen om de folder te verwijderen  Alle onderliggende folders, keys en bestanden verwijderd. |
| Web | [NIET ONDERSTEUND]  Kies een hoofdfolder.  Folder en onderliggende folders,keys en bestanden worden verwijderd. |

## Verplaatsen bestand naar andere hoofdfolder of subfolder daarvan

|  |  |
| --- | --- |
| Device | Gebruiker selecteert bestand en target folder.  Bestand wordt gedownload  Bestand wordt onversleuteld met key source folder (mits hoofdfolder versleuteld)  Bestand wordt versleuteld met key taget folder (mist hoofdfolder versleuteld)  Bestand wordt geupload  Bestand verwijderen uit source folder verwijderen via API  Bestand verwijderen lokaal |
| Sync | Sync detecteert move.  Bestand wordt versleuteld met key taget folder (mits hoofdfolder versleuteld)  Bestand wordt geupload  Bestand verwijderen uit source folder verwijderen via API |
| Web | Verplaatsen kan alleen in onbeveiligde folders |

## Updaten van een bestand

|  |  |
| --- | --- |
| Device | Gebruiker past bestand en kiest voor uploaden.  Bestand wordt versleuteld met juiste key. |
| Sync | Gebruiker update bestand.  Sync detecteert update  Key wordt opgehaald.  Bestand wordt versleuteld  Bestand wordt geupload. |
| Web | [NIET ONDERSTEUND]  Gebruiker selecteert bestand kiest nieuwe versie.  Gebruiker geeft pass-phrase  Bestand wordt gupload  Bestand wordt versleuteld met juiste key van folder. |

# Bestaande API Overzicht

De documentatie over de API’s die gebruikt worden staan op de volgende locatie:

http(s)://[localbox]/api/doc