



QUICK
Technology

Save time,
not passwords.



QUICK Technology

Save **time**,
not **passwords**.

Cryptshare QUICK Technology is een revolutie in de veiligheid bij verzending van uw gegevens. Een krachtige innovatie die helemaal voldoet aan uw digitale beveiligingseisen en binnen enkele seconden een permanente en veilige verbinding mogelijk maakt. Na activering verzorgt QUICK alle wachtwoorden tussen de communicatiepartners, beveiligt de gegevensoverdracht en bespaart ook nog kostbare tijd. Bedieningsgemak wordt gecombineerd met beveiliging van gegevensoverdracht en bedrijven kunnen e-mail, een van de bekendste

communicatiemiddelen, gebruiken om met iedereen te communiceren: klanten, bedrijven of leveranciers. QUICK vergemakkelijkt de almaar toenemende veiligheidseisen aan uw communicatie en stelt u in staat om onmiddellijk ideeën en kennis met anderen te delen.

Cryptshare QUICK Technology – save time, not passwords.

Waarom is
**wachtwoord-
beveiliging**
zo belangrijk?

Wachtwoordbeveiliging is essentieel voor uw communicatie in het digitale tijdperk. Het regelt de encryptie tussen afzender en ontvanger en beschermt daardoor uw gegevens op alle mogelijke locaties. Bedrijfsspionage en professionele hackers zijn constante bedreigingen waartegen alle bedrijven zich moeten wapenen en het misbruik van wachtwoorden en slecht wachtwoordbeheer zijn de belangrijkste oorzaken van veel datalekken. Het opzetten en onderhouden van wachtwoordbeveiliging vraagt echter altijd extra inspanning: wachtwoorden

moeten worden gegenereerd en vervolgens worden uitgewisseld tussen de communicatiepartners - voor elke afzonderlijke gegevensoverdracht. Een moeizame en tijdrovende klus. Om die reden wordt bedieningsgemak vaak verkozen boven de veiligheid van de uit te wisselen gegevens:

Nadat een wachtwoord eenmaal is ingesteld, wordt het vaak permanent gebruikt bij de uitwisseling tussen twee communicatiepartners en soms zelfs gebruikt in andere toepassingen.

iq086-Y
1b2ctf4
P02334f

@=I#14)I

sAt;Do)
F6ibAd?

1-#-2dE?
sAt;Do)
ZqKye1xk
UoV(O#%oc

\$F6ibAd?

n9s%JBx2
V6,34G;n
-z7!K;;ib
du8isgun

UoV(O#%oc

2yecVnT&
qi,0qZo:

#QzRJ9cl
n2W=1V;4
Yd*peG3R
.98jex%os

uB5zhu~B

6(+o@L4i

n-CfuW+o

U]zbechR

2ybTz11 266C

Yd*peG3R
#QzRJ9cl

ZqKye1xk

godU9/8U

5E!QFZT7

CsAt;Do)
ZqKye1xk

godU9/8U

6EMQuK,a

p1s~@A4

\$F6ibAd?
UoV(O#%oc

CsAt;Do)
ZqKye1xk

godU9/8U

5E!QFZT7

p1s~@A4

5E!QFZT7

Yd*peG3R
.98jex%os

@=I#14)I

n9s%JBx2

#QzRJ9cl

uB5zhu~B

6(+o@L4i

qi,0qZ

qi,0
UoV

Z
A





Hoe hebben we Cryptshare nog geschikter en gebruiksvriendelijker gemaakt voor regelmatige uitwisseling tussen dezelfde communicatiepartners en hoe hebben we het probleem van beveiliging van de gegevensoverdracht opgelost? Met QUICK Technology natuurlijk. Aangezien Cryptshare geen gebruikersaccounts of certificaten vereist, wilden we ons cryptografische uitgangspunt handhaven - en dat hebben we ook gedaan. QUICK gebruikt in eerste instantie een eenmalig wachtwoord en voor alle verdere communicatie tussen afzender en ontvanger worden nieuwe wachtwoorden gebruikt, zonder dat gebruikers verder nog iets hoeven te doen. Het elimineert de noodzaak om nieuwe wachtwoorden uit te wisselen tussen afzender en ontvanger of te vertrouwen op statische sleutelparen die altijd kwetsbaar zijn. Met QUICK worden deze versleutelde wachtwoorden automatisch gegenereerd aan verzenderszijde en kunnen ze automatisch worden herkend aan ontvangerszijde. Zodra QUICK

geactiveerd is, hoeven gebruikers zich niet meer bezig te houden met wachtwoorden. Zodra de permanente en veilige verbinding tot stand is gebracht, kan alle informatie ongeacht type en omvang veilig via e-mail worden uitgewisseld. Gebruikers hoeven niet langer wachtwoorden te onthouden of te hergebruiken voor toekomstige gegevensoverdrachten. U kunt QUICK zelf activeren, daar is geen diepgaand technisch inzicht voor nodig. Er is geen hulp van een systeembeheerder nodig en er hoeft niet aan speciale IT-vereisten te worden voldaan. Cryptshare is geschikt voor alle medewerkers, ongeacht hun computerkennis. Als gevolg hiervan worden: kosten sterk gereduceerd, is de uitrol snel en eenvoudig is de gebruikersbeleving uniform en is het bedrijf veiliger.

QUICK Technology brengt een revolutie teweeg in de uitwisseling van informatie door beveiliging van gegevensoverdracht in harmonie te brengen met gebruiksvriendelijkheid. Alle extra handelingen voor gebruikers zijn geëlimineerd.

Waarom is **wachtwoord- beveiliging** zo belangrijk?

Meer technische informatie
vindt u hier:

wiki.cryptshare.com/quick



User-to-user

Voor verzekeringsmaatschappijen is het bijvoorbeeld belangrijk om bereikbaar te zijn voor klanten. Of het nu gaat om schadeclaims of andere vragen, mensen moeten te allen tijde gelegenheid hebben om contact op te nemen met hun verzekeringsmaatschappij. Dit geldt evenzeer voor de omgekeerde richting: ook als het gaat om polis- of premiewijzigingen hebben verzekeraars een betrouwbaar kanaal nodig om hun verzekeringsnemers te bereiken. Meestal gaat het bij dergelijke communicatie om dringende zaken en uiterst gevoelige privégegevens. Het is van het grootste belang dat verzekeringsmaatschappijen gebruik

maken van een communicatiekanaal dat de integriteit van uitgewisselde gegevens beveiligd en waarborgt, en informatie snel doorstuurt naar communicatiepartners. Dat is nou precies wat QUICK mogelijk maakt: een permanent en veilig communicatiekanaal zonder beperkingen in bestandsgrootte. Gevoelige informatie kan bidirectioneel, veilig en spontaan worden verzonden. Gebruikers hebben geen derden of diepgaande technische kennis nodig. Met QUICK kunnen organisaties via e-mail een permanente en directe communicatie met hun klanten realiseren. Snel, probleemloos en voordelig.

Machine-to-user

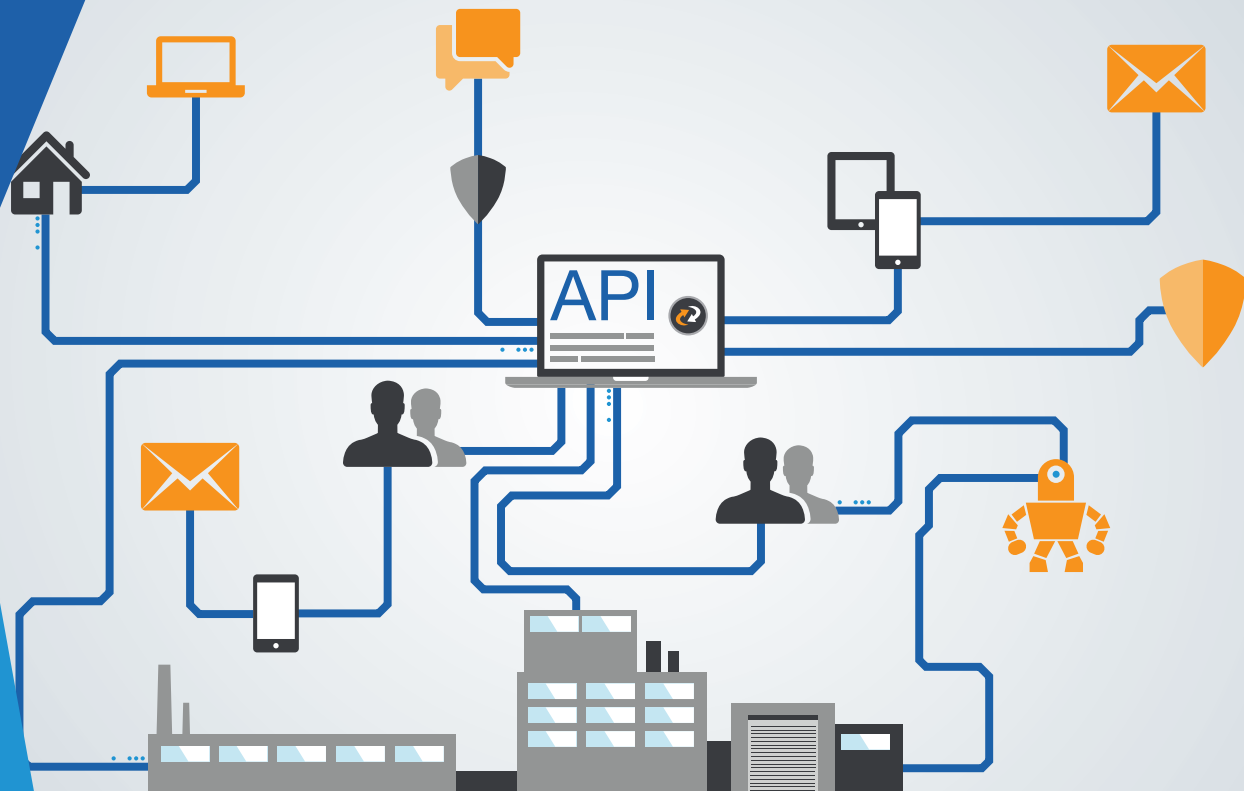
Voor banken is bijvoorbeeld de veilige en vertrouwelijke uitwisseling van gevoelige gegevens van cruciaal belang bij zowel interne als externe communicatie. Kredietaanvragen, hypotheekdocumenten en kredietwaardigheid zijn uiterst gevoelige informatie en zowel bestaande als potentiële nieuwe klanten willen zekerheid dat hun gegevens veilig worden uitgewisseld. De gebrekkige gebruiksvriendelijkheid van de meeste systeemoplossingen vormt echter een belemmering

voor klanten en is een drempel in de communicatie tussen banken en de buitenwereld. QUICK neemt deze drempel weg. Het stelt elke organisatie in staat om regelmatige communicatie te onderhouden via een permanente en veilige verbinding die ongeëvenaard is in gebruiksvriendelijkheid: geen gebruikersaccounts, geen extra software, geen gedoe. Klanten kunnen vertrouwen op het medium dat zij het beste kennen: e-mail.

```
elif operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0
done = bpy.context.selected_objects[0]
#bpy.data.objects[mirror_ob.name].select = 0

print("Please select exactly two objects, the last one gets deleted")
```



Geautomatiseerde technologie helpt in toenemende mate om financiële middelen te besparen en werkprocessen efficiënter te maken. Het beveiligen van geautomatiseerde processen, vooral bij omgang met gevoelige gegevens, is essentieel om het volledige potentieel van technologie te kunnen benutten. Bij genetische tests, bijvoorbeeld, kan medische apparatuur stalen analyseren en de resultaten omzetten in bestanden. Deze bestanden kunnen vervolgens naar medische instellingen worden

gestuurd, waar ze automatisch worden opgeslagen en voor verdere verwerking worden toegewezen aan specifieke medewerkers. Met QUICK kan communicatie vanaf medische apparatuur met zeer gevoelige gegevens, permanent worden beveiligd. Door de invoering van innovatieve wachtwoordbeveiliging versterkt QUICK de integriteit van geautomatiseerde processen en verruimt het toepassingspectrum door verbeterde efficiëntie en traceerbaarheid.

Machine-to-machine

E-mail is een universele standaard en zal in de nabije toekomst waarschijnlijk niet zomaar verdwijnen.

Daarom zijn Cryptshare en QUICK Technology ontwikkeld om nauw

samen te werken met uw bestaande e-mailsysteem. De bekende problemen van e-mail zijn opgelost door Cryptshare - QUICK Technology is de kers op de taart die voor absolute gebruiksvriendelijkheid zorgt.

Hoe werkt dit samen met **andere technologieën?**

Welke voordelen heeft QUICK?

Voor het tot stand brengen van permanente veilige verbindingen, vereisen verouderde technologieën gewoonlijk dat gebruikers of een goed wachtwoordbeheer implementeren, opzetten en onderhouden, of certificaten kopen en (publieke) sleutels uitwisselen.

Goed wachtwoordbeheer is een voorwaarde voor sterke gegevensbeveiliging tijdens het versturen, wat betekent dat voor elke overdracht een uniek wachtwoord moet worden gebruikt. Deze wachtwoorden moeten niet alleen worden aangemaakt, maar moeten ook worden uitgewisseld tussen de communicatiepartners. Het wordt aanbevolen om dit te doen via een communicatiekanaal dat gescheiden is van de e-mail.

In de praktijk leidt goed wachtwoordbeheer echter tot aanzienlijke inspanningen voor gebruikers. Het is erg tijdrovend om wachtwoorden uit te wisselen voor elke overdracht. Communicatie is niet langer spontaan, maar kan ernstig vertraagd worden als de ontvanger bijvoorbeeld niet telefonisch bereikbaar is om het wachtwoord voor de aanstaande overdracht te geven. Om die redenen kiezen gebruikers meestal voor gemak boven beveiliging

en gebruiken ze daarom slechts zeer weinig verschillende wachtwoorden voor gegevensuitwisseling met hun communicatiepartners. Heel vaak gebruiken ze slechts maar één. Dit brengt de beveiliging van hun communicatie ernstig in gevaar en geeft hackers de ruimte om aan te vallen.

Het gebruik van certificaten voor het beveiligen van uw gegevens tijdens het versturen is duur. Ze moeten worden aangeschaft, hebben een beperkte levensduur en moeten uiteindelijk worden vernieuwd. Er zijn ook extra kosten voor beheer van dit soort certificaten, namelijk onderhoud, omgaan met verloren certificaten en met vergeten wachtwoorden, enz. Bovendien vereist het uitwisselen van (publieke) sleutels behoorlijk veel technische expertise. De meeste gebruikers kunnen dit niet zelf, maar vertrouwen op een beheerder om dit voor hen te doen. Dit betekent dat ze voor elke nieuwe beveiligde verbinding met een communicatiepartner afhankelijk zijn van de beheerder en moeten wachten tot een derde de nodige stappen uitvoert. Afgezien van de bijkomende kosten, elimineert dit elk spontaan element en vertraagt het de communicatie.

QUICK combineert gegevensbeveiliging met gebruiksgemak. Het vereist geen software, omdat het nauw samenwerkt met bestaande e-mailprogramma's, of een speciale IT-infrastructuur voor het beheren of onderhouden van codesleutels. Als gevolg hiervan worden de kosten voor de verzender en de ontvanger aanzienlijk verlaagd. Sterker nog, externe communicatiepartners hebben helemaal geen kosten! QUICK is opgenomen (zonder extra kosten) in de reguliere Cryptshare-update. Gebruikers kunnen QUICK in slechts enkele seconden zelf activeren wanneer dit nodig is waardoor ze waardevolle tijd besparen. Wachtwoordbeheer is niet langer vereist, aangezien QUICK permanent beveiligde verbindingen tot stand brengt en alle wachtwoordproblemen voor gebruikers oplost.

Maar dit zijn niet de enige voordelen die QUICK in huis heeft. Het versterkt ook de relaties van gebruikers met hun communicatiepartners door een regelmatige en intensieve communicatie per e-mail mogelijk te maken. QUICK biedt permanent beveiligde verbindingen voor alle gegevensuitwisselingen en is gemakkelijk en spontaan te gebruiken.





Gegevensoverdracht, permanent beveiligd. Voor degenen die hun communicatie willen beveiligen en AVG-conform willen maken, regelt Cryptshare de encryptie zonder beperkingen in bestandsgrootte op een kosteneffectieve manier. Met QUICK, dat onderdeel is van de nieuwste Cryptshare-versie, wordt Security by Design naar een heel nieuw niveau getild, omdat veilige gegevensuitwisseling door het opzetten van permanent veilige verbindingen nu eenvoudiger is dan ooit. **Geen problemen en ergernissen meer met wachtwoorden.** Eenmaal geactiveerd, regelt QUICK de

wachtwoorden voor elke toekomstige uitwisseling tussen u en uw communicatiepartner. Permanent en zonder extra kosten. Uw gegevensoverdracht is altijd veilig.

Beveiliging (weer) gemakkelijk gemaakt. QUICK is eenvoudig in gebruik en permanent veilige verbindingen zijn met slechts enkele klikken opgezet. U kunt dit op elk moment activeren, QUICK is klaar wanneer u het nodig heeft. Geen beheerders of technische deskundigheid nodig.

QUICK brengt een permanent veilige verbinding tot stand voor de gegevens van communicatiepartners die worden verstuurd, terwijl het alle extra handmatige inspanningen voor gebruikers elimineert. Hoe werkt het? Tijdens de eerste QUICK-overdracht tussen twee deelnemers wordt automatisch een gedeelde sleutel gemaakt en op de server opgeslagen. Deze is alleen toegankelijk met behulp van een lokaal element dat automatisch wordt uitgegeven voor geverifieerde gebruikers door de server en opgeslagen op de computer van de gebruiker. Deze gedeelde sleutel wordt gebruikt om unieke en willekeurig eenmalige wachtwoorden af te leiden voor elke overdracht. Deze

individueel eenmalige inloggegevens worden vervolgens gebruikt om alle gegevens en bestanden van specifieke overdrachten te coderen en te decoderen. De ontvanger kan deze wachtwoorden automatisch afleiden en toepassen zonder ze met de afzender te hoeven uitwisselen, terwijl elke overdracht tussen afzender en ontvanger wordt beschermd door het zeer veilige eenmalige wachtwoord. Zodra deze permanent beveiligde verbinding tot stand is gebracht, hoeven gebruikers in de toekomst geen wachtwoorden meer te onthouden of te gebruiken. Het duurt slechts enkele seconden. Cryptshare QUICK Technology. Save time, not passwords.

Waarom heb ik **QUICK** nodig?

Hoe werkt het voor de gebruiker vanuit een meer technisch oogpunt?

Over Cryptshare

Cryptshare biedt een korte termijn effect op basis van een lange termijn oplossing voor de beveiliging van e-mail communicatie. Of het nu gaat om de beveiliging van de inhoud van de mail of dat de mail veilig een groot bestand moet versturen. Cryptshare zorgt dat er wordt voldaan aan geldende wet-en regelgeving, maakt e-mail verkeer traceerbaar en beheersbaar, kostenefficiënt en grondig. Cryptshare - Secure all the way.

Hoe is het allemaal begonnen?

Cryptshare AG is in 2000 opgericht als gespecialiseerde ontwikkelaar van maatwerksoftware in opdracht van verschillende 'Blue Chip' klanten. Zo werden de afgelopen jaren meerdere oplossingen ontwikkeld die, met beperkte aanpassingen, bij meerdere klanten goed bruikbaar bleken. Gevolg was dat we daarmee meerdere klanten konden bedienen met stabiele en bewezen functionaliteit, goed bruikbaar voor het oplossen van complexe bedrijfsprocessen. Daarmee zijn wij ervan overtuigd dat onze producten problemen oplossen waar andere oplossingen dat niet kunnen.

De ontwikkeling van Cryptshare

Cryptshare werd in 2007 uitgeleverd aan de eerste klanten. Dit zorgde direct voor meerdere aanvragen van andere klanten. Het bleek al snel dat het adhoc uitwisselen van grote bestanden en het beveiligen van e-mailcommunicatie steeds belangrijker werd voor zowel kleinere als grotere bedrijven in diverse branches.

Feedback uit de markt en een sterk vertrouwen in het team zorgde voor het ontstaan van onze roadmap. Aan de hand van de vragen uit de groeiende klantengroep, werden nieuwe functionaliteiten aan Cryptshare toegevoegd. Zo werden zaken als gebruiksvriendelijkheid, krachtige encryptie en geavanceerde managementfuncties toegevoegd. Dit werd aangevuld met configuratie- en policy tools en de mogelijkheid om met andere softwareapplicaties te koppelen op basis van API's.

Cryptshare nu

Sinds 2010 is aantal klanten sterk gegroeid. Doordat we in veel landen met meerdere resellers werken kunnen we snel schakelen met de verkoop van Cryptshare. Met het uitbreiden van het aantal medewerkers is de realisatie van de roadmap op een hoger niveau gebracht. Dankzij de extra medewerkers op de Support afdeling hebben we meer verkopen marketing activiteiten mogelijk gemaakt. Op dit moment heeft Cryptshare meer dan 4 miljoen gelicenseerde klanten in 30 verschillende landen.

“De Gemeente Zaanstad is een gemeente met ruim 150.000 inwoners. De toename in het delen van informatie tussen verschillende organisaties zorgde ervoor dat we op zoek moesten naar een gebruiksvriendelijke oplossing waarbij we vertrouwelijke informatie via email konden versturen. Een oplossing zonder extra drempels als een extra login. Met Cryptshare hebben we nu een betrouwbare applicatie geïmplementeerd. Hiermee kunnen we, direct vanuit Outlook, vertrouwelijke data met behulp van een encryptie per mail versturen.

We kenden een slow start maar momenteel wordt Cryptshare dagelijks gebruikt binnen onze organisatie.”

Linda Goedhart, ICT Adviseur
Gemeente Zaanstad



Cryptshare AG

Schwarzwaldstr. 151
79102 Freiburg
Germany

Phone: +49 761 / 38913-0
Fax: +49 761 / 38913-115
E-mail: info@cryptshare.com
Web: www.cryptshare.com

Register Court Freiburg, HRB 6144

CEO: Mark Forrest, Dominik Lehr
Chairman: Thilo Braun

VAT-ID: DE812922179

© 2019 Cryptshare AG.

-  Email encryptie
-  Ongelimiteerde bestandsgrootte
-  Volledig traceerbaar