HIRSCH

FAQ SECUREKEY & SECUREPASS

Häufig gestellte Fragen zu FIDO2, PIV, OTP und PGP

AUTHENTIFIZIERUNG



INHALT

01	Erste Schritte	F01–F05
02	Kompatibilität	F06–F12
03	Nutzung von SecureKey und SecurePass	F13–F19
04	Fehlerbehebung	F20–F21
05	FIDO2 & passwortlose Authentifizierung	F22–F33
06	Unternehmen & On-Premises	F34–F41
07	PIV-Authentifizierung (Smartcard)	F42–F51
08	OTP-Authentifizierung (HOTP)	F52–F56
09	PGP-Verschlüsselung	F57–F67

DIE + PUNKTE

- **SOFORT EINSATZBEREIT** – Für FIDO2 ist keine Konfiguration nötig; die PIN wird bei der ersten Registrierung festgelegt.
- **KEINE TREIBER** – Funktioniert ohne Treiberinstallation an Computern, Tablets und Smartphones.
- **PHISHINGRESISTENT** – Anmeldeinformationen sind an die Website gebunden und verlassen das Gerät nie.
- **PLATTFORMÜBERGREIFEND** – Windows, macOS, Linux, iOS und Android über USB-A, USB-C oder NFC.
- **BACKUP-SCHLÜSSEL** – Pro Konto einen zweiten Schlüssel registrieren, damit ein Verlust nie zur Aussperrung führt.

01 ERSTE SCHRITTE

F01
Was ist FIDO2 und wie funktioniert SecureKey bzw. SecurePass?

FIDO2 ist ein offener Authentifizierungsstandard der FIDO Alliance, der Passwörter durch Public-Key-Kryptografie ersetzt. SecureKey bzw. SecurePass ist ein Hardwaregerät, das Ihre privaten Schlüssel erzeugt und speichert. Die Anmeldung erfolgt einfach per Berührung, PIN oder NFC-Antippen.

F02
Warum sollte ich SecureKey oder SecurePass statt eines Passworts verwenden?

Passwörter können per Phishing abgegriffen, mehrfach verwendet oder gestohlen werden. SecureKey bzw. SecurePass erzeugt mittels Public-Key-Kryptografie für jedes Konto eine eigene Anmeldeinformation. Es gibt also kein gemeinsames Geheimnis, das ein Angreifer stehlen könnte – Ihr privater Schlüssel verlässt das Gerät nie.

F03
Was ist ein Passkey und worin unterscheidet er sich von SecureKey bzw. SecurePass?

Ein Passkey ist die Anmeldeinformation selbst – ein öffentliches/privates Schlüsselpaar, das nach dem Standard FIDO2/WebAuthn erzeugt wird. SecureKey bzw. SecurePass ist das physische Gerät, das Passkeys erzeugt und speichert. SecureKey und SecurePass unterstützen außerdem PIV und OTP. „SecureKey“ bzw. „SecurePass“ bezeichnet also das Gerät, „Passkey“ dagegen speziell eine FIDO2-Anmeldeinformation.

F04
Wie beginne ich mit meinem neuen SecureKey bzw. SecurePass?

Registrieren Sie den Schlüssel direkt bei dem Konto, das Sie schützen möchten (z. B. Microsoft, Google, Ihre Bank) – eine vorherige Registrierung bei Hirsch ist nicht nötig. Wählen Sie in den Sicherheitseinstellungen des Kontos „Sicherheitsschlüssel einrichten“, stecken Sie den Schlüssel ein bzw. halten Sie ihn an das Gerät und folgen Sie den Anweisungen. Anleitungen für einzelne Anwendungen finden Sie auf der Hirsch-Seite „Works with SecureKey and SecurePass“.

F05
Muss ich SecureKey bzw. SecurePass vor der Nutzung mit FIDO2 konfigurieren?

Nein. Für FIDO2 sind die Schlüssel sofort einsatzbereit; die meisten Dienste fordern Sie bei der ersten Registrierung lediglich auf, eine PIN festzulegen. Eine Konfiguration ist nur nötig, wenn Sie zusätzlich die PIV- oder OTP-Applets nutzen möchten.

02 KOMPATIBILITÄT

F06
Welche Geräte und Betriebssysteme werden unterstützt?

SecureKey und SecurePass funktionieren je nach Modell mit Windows, macOS, Linux, iOS und Android über USB-A, USB-C oder NFC. Prüfen Sie, ob Ihr Gerät über einen passenden Anschluss oder NFC verfügt.

F07
Welche Browser unterstützen FIDO2-Sicherheitsschlüssel?

Browser	Betriebssystem	Unterstützung
Chrome	Windows / Mac / Linux	FIDO2 & U2F
Firefox	Windows / Mac / Linux	FIDO2 & U2F
Edge	Windows	FIDO2
Opera	Windows / Mac / Linux	FIDO2 & U2F
Safari	macOS / iOS	FIDO2 & U2F

F08
Funktioniert das mit meinem iPhone?

Ja, mit jedem NFC-fähigen iPhone – das sind die meisten Modelle der letzten Jahre.

F09 **Funktioniert das mit meinem Chromebook?**	Ja, sofern ChromeOS aktuell ist, Sie einen unterstützten Browser verwenden und Ihr Chromebook einen USB-Anschluss hat.
F10 **Kann ich SecureKey oder SecurePass mit meiner Apple-ID verwenden?**	Ja. SecureKey und SecurePass funktionieren je nach Gerät über USB-A, USB-C oder NFC mit der Apple-ID.
F11 **Ist SecureKey bzw. SecurePass mit Microsoft Entra ID / Azure kompatibel?**	Ja. SecureKey und SecurePass werden von Microsoft Entra ID nativ für die passwortlose Anmeldung bei Microsoft 365 und anderen mit Azure verbundenen Anwendungen unterstützt.
F12 **Mein Mac fordert mich auf, Tasten zu drücken, um den Tastaturtyp zu erkennen – funktioniert mein Schlüssel noch?**	Ja. Das ist die übliche Tastaturerkennung von macOS und hat nichts mit Ihrem Schlüssel zu tun. Schließen Sie das Fenster und fahren Sie fort; der Schlüssel funktioniert normal.

03 NUTZUNG VON SECUREKEY UND SECUREPASS

F13
Wie viele Konten kann ein SecureKey bzw. SecurePass schützen?

Modell	Kapazität residenter Schlüssel (Credential-Slots) gesamt	Max. residente Schlüssel pro Relying Party (RP)
SecureKey	32	32
SecureKey GOV und SecurePass	40	10

F14 **Brauche ich für jede Anwendung oder jedes Gerät einen eigenen SecureKey bzw. SecurePass?**	Nein. Ein SecureKey bzw. SecurePass kann bei mehreren FIDO2/U2F-zertifizierten Anwendungen registriert und auf mehreren Geräten genutzt werden, sofern jedes Gerät einen kompatiblen Anschluss oder NFC hat.
F15 **Was passiert, wenn ich meinen SecureKey bzw. SecurePass verliere – bin ich dann dauerhaft ausgesperrt?**	Das hängt vom Dienst ab; die meisten bieten Wiederherstellungsoptionen wie Backup-Codes oder eine alternative Verifizierung. Empfehlenswert ist, pro Konto zwei Schlüssel zu registrieren – einen Haupt- und einen Ersatzschlüssel –, damit Sie bei Verlust nie ausgesperrt sind.
F16 **Kann ich meinen SecureKey bzw. SecurePass als Backup duplizieren?**	Nein, das sichere Hardwaredesign verhindert eine Duplizierung. Registrieren Sie stattdessen bei jedem Konto einen zweiten physischen Schlüssel als Backup.
F17 **Bin ich nach der Registrierung dauerhaft an diesen Schlüssel gebunden?**	Nein. Sie können registrierte Schlüssel jederzeit zu Ihrem Konto hinzufügen oder daraus entfernen.
F18 **Muss ich Treiber installieren?**	Nein. SecureKey und SecurePass funktionieren ohne Treiberinstallation an Computern, Tablets und Smartphones.
F19 **Ist ein SecureKey bzw. SecurePass wirklich „Multi-Faktor“, wenn es nur ein Schlüssel ist?**	Ja. Bei der Registrierung legen Sie zusätzlich eine PIN fest. Der Schlüssel ist „etwas, das Sie besitzen“, die PIN „etwas, das Sie wissen“ – zusammen erfüllen sie die Anforderungen an eine Zwei-Faktor-Authentifizierung.

04 FEHLERBEHEBUNG

F20 **Mein Schlüssel wird nicht erkannt, die Registrierung schlägt fehl oder es kommt zu einer Zeitüberschreitung – was sollte ich prüfen?**	■ Schlüssel erneut einstecken; bei USB-A auf die richtige Ausrichtung achten und vollständig einstecken. ■ Einen anderen Anschluss, ein anderes Gerät oder einen unterstützten Browser (Chrome, Firefox, Edge, Safari) verwenden. ■ Den Schlüssel bei Aufforderung zügig berühren bzw. antippen – die meisten Zeitüberschreitungen entstehen, weil der Schlüssel nicht schnell genug aktiviert wird. ■ Ist für das Konto bereits eine Anmeldeinformation vorhanden, diese vor der erneuten Registrierung entfernen, um den Fehler „doppelte Anmeldeinformation“ zu vermeiden. ■ Schlägt die Verifizierung fehl, prüfen, ob die richtige PIN eingegeben wird. ■ Mit dem Hirsch uTrust Key Manager Modell, Firmware und FIDO2-Unterstützung des Schlüssels prüfen.
F21 **Ein Browser meldet „nicht kompatibel mit WebAuthn“ – was bedeutet das?**	Ihr Browser bzw. dessen Version unterstützt FIDO2 nicht. Wechseln Sie zur aktuellen Version von Chrome, Firefox, Edge oder Safari (siehe Abschnitt Kompatibilität).

05 FIDO2 & PASSWORTLOSE AUTHENTIFIZIERUNG

F22 **Was ist der Unterschied zwischen FIDO U2F und FIDO2?**	FIDO U2F (2014) ist ein zweiter Faktor, der zusätzlich zum Passwort verwendet wird. Das neuere FIDO2 (2019) ermöglicht eine vollständig passwortlose Authentifizierung: Eine PIN oder ein biometrisches Merkmal entsperrt den Schlüssel lokal, und es wird nie ein Geheimnis an den Onlinedienst übertragen.
F23 **Warum schützt FIDO2 meine Konten besser als ein Passwort?**	Jedes Konto erhält ein eigenes, auf dem Gerät erzeugtes Schlüsselpaar. Der private Schlüssel verlässt Ihren Schlüssel nie und wird vom Dienst weder empfangen noch gespeichert. Damit entfallen die Risiken durch Phishing, Credential Stuffing und Passwort-Wiederverwendung. Ein gestohlener Schlüssel allein reicht nicht aus – ein Angreifer bräuchte zusätzlich Ihre PIN oder Ihr biometrisches Merkmal.
F24 **Wenn ich denselben Schlüssel auf mehreren Websites nutze, kann eine Website erkennen, dass ich ihn auch anderswo verwende?**	Nein. Jede Website erhält eine separate, eindeutige Anmeldeinformation, und FIDO2 erlaubt es Websites nicht, Ihre Aktivitäten dienstübergreifend zu verknüpfen.
F25 **Gibt FIDO2 persönliche Daten an Websites oder die FIDO Alliance weiter?**	Nein. Die FIDO Alliance definiert nur den Standard und erhebt keine Daten. Ihre Anmeldeinformationen bleiben auf Ihrem Gerät; außer dem öffentlichen Schlüssel wird nichts an Anbieter oder Dienste weitergegeben.
F26 **Warum kann eine Phishing-Website meinen Schlüssel nicht zur Authentifizierung verleiten?**	FIDO2-Anmeldeinformationen sind kryptografisch an die Herkunft (Origin) der Website gebunden. Eine für eine Website erstellte Anmeldeinformation kann daher auf einer nachgeahmten Phishing-Website nicht verwendet werden – auch nicht von einem Angreifer.

F27 **Was ist der Unterschied zwischen einem Plattform-Authenticator und einem Roaming-Authenticator wie meinem uTrust-Schlüssel?**	Ein Plattform-Authenticator (z. B. Windows Hello, Touch ID) ist in Ihr Gerät integriert. Ein Roaming-Authenticator wie ein uTrust-Schlüssel ist ein externes Gerät, das Sie mitnehmen und an mehreren Computern verwenden können.
F28 **Was ist NFC-FIDO und wie nutze ich es?**	Mit NFC-fähigen uTrust-Schlüsseln authentifizieren Sie sich drahtlos: Halten Sie den Schlüssel einfach an Ihr Smartphone, Tablet oder einen NFC-fähigen Leser, statt ihn einzustecken.
F29 **Wenn ich einen Schlüssel unter Windows registriere, funktioniert er dann auch auf meinem Mac?**	Ja. FIDO2-Anmeldeinformationen sind an Ihr Konto gebunden, nicht an das Betriebssystem. Derselbe Schlüssel funktioniert daher plattformübergreifend, sofern der Dienst FIDO2/WebAuthn auf beiden Plattformen unterstützt.
F30 **Kann ich einen Passkey von einem SecureKey bzw. SecurePass auf einen anderen übertragen oder in Samsung Vault speichern?**	Nein. Jeder Schlüssel erzeugt pro Konto eine eigene, eindeutige Anmeldeinformation, die sich nicht zwischen Hardwareschlüsseln kopieren oder übertragen lässt. Registrieren Sie als Backup einen zweiten Schlüssel separat beim selben Konto. Samsung Vault speichert softwarebasierte Passkeys, keine Anmeldeinformationen von externen Hardwareschlüsseln.
F31 **Was ist der Unterschied zwischen einem gerätegebundenen Passkey (SecureKey bzw. SecurePass) und einem synchronisierten Passkey (z. B. iCloud-Schlüsselbund)?**	Gerätegebundene Passkeys befinden sich ausschließlich auf dem physischen Schlüssel und verlassen ihn nie – das maximiert die Sicherheit. Synchronisierte Passkeys werden aus Bequemlichkeit über einen Cloud-Dienst auf Ihre Geräte kopiert, wodurch die Anmeldeinformation stärker exponiert ist. SecureKey und SecurePass verwenden gerätegebundene Passkeys.
F32 **Wie melde ich mich mit meinem FIDO2-Schlüssel an?**	Wählen Sie bei der Anmeldung „Sicherheitsschlüssel“ oder „Passkey“, stecken Sie Ihren Schlüssel ein bzw. halten Sie ihn an das Gerät und schließen Sie den Vorgang ab – meist durch Berühren und/oder PIN-Eingabe.
F33 **Wie lege ich die PIN meines FIDO2-Schlüssels fest oder ändere sie?**	Die meisten Dienste fordern Sie zur Festlegung einer PIN auf, sobald erstmals eine Verifizierung nötig ist. Sie können die PIN auch mit dem Hirsch uTrust Key Manager festlegen oder ändern oder unter Windows über Einstellungen → Konten → Anmeldeoptionen → Sicherheitsschlüssel.
06 UNTERNEHMEN & ON-PREMISES-AUTHENTIFIZIERUNG	
F34 **Welche Rolle kann ein SecureKey GOV in hybriden Umgebungen (Cloud + On-Premises) spielen?**	Der GOV-Schlüssel vereint FIDO2 für die passwortlose Cloud-Anmeldung mit einem PIV/PKI-Applet für die zertifikatsbasierte On-Premises-Authentifizierung – in einem einzigen nach FIPS 140-3 validierten, TAA-konformen Gerät. So kann ein Schlüssel sowohl Cloud- als auch On-Premises-Identitätssysteme bedienen.
F35 **Wann sollte ich PKI (X.509-Zertifikate) statt FIDO2 verwenden?**	PKI/PIV ist für Legacy- oder infrastrukturbasierte Anwendungsfälle vorzuziehen, etwa die Anmeldung an einer Active-Directory-Domäne, RDP-Sitzungen und Thin-Client-Umgebungen, in denen bereits zertifikatsbasiertes Vertrauen besteht. FIDO2 eignet sich am besten für die Anmeldung an Cloud- und Webanwendungen.
F36 **Wie aktiviere ich FIDO2 für die lokale Windows-Anmeldung (On-Premises)?**	Nutzen Sie die Lösung Hirsch uTrust Windows Logon. Sie stellt eine lokale Middleware bereit, mit der sich Benutzer mit einem FIDO2-Schlüssel passwortlos an Windows-Arbeitsplätzen anmelden.

F37 **Unterstützt der uTrust FIDO2 Login Manager Active Directory?**	Der Login Manager übernimmt nur die Anmeldung am lokalen Rechner und ist nicht in Active-Directory-Authentifizierungsabläufe eingebunden. Für die AD-Domänenanmeldung verwenden Sie stattdessen die PIV-basierte Smartcard-Authentifizierung.
F38 **Wie nutze ich SecureKey oder SecurePass für die Active-Directory-Domänenanmeldung?**	Spielen Sie über die PKI Ihrer Organisation (z. B. AD-Zertifikatdienste) ein PIV-Authentifizierungszertifikat auf das PIV-Applet des Schlüssels auf. Der Schlüssel funktioniert dann wie eine Standard-PIV-Smartcard für die AD-Anmeldung.
F39 **Ist ein SecureKey bzw. SecurePass mit FIPS 140-3 für den Unternehmenseinsatz einer Smartcard gleichwertig?**	Funktional ja. FIPS-140-3-Schlüssel mit PIV-Applet unterstützen die zertifikatsbasierte Authentifizierung genauso wie eine Smartcard – nur in einem anderen Formfaktor.
F40 **Wie fügt sich FIDO2 in Microsoft Entra ID / Office 365 ein?**	FIDO2 wird von Microsoft Entra ID nativ für die passwortlose Anmeldung bei Microsoft 365 und anderen mit Azure verbundenen Anwendungen unterstützt.
F41 **Müssen wir SecureKey bzw. SecurePass vorkonfigurieren, bevor wir sie an Benutzer ausgeben?**	Für FIDO2 nicht – die Benutzer registrieren ihren Schlüssel selbst bei jedem Dienst. PIV-Zertifikate können Sie jedoch auf Wunsch vorab aufspielen.

07 PIV-AUTHENTIFIZIERUNG (SMARTCARD)

F42 **Was ist PIV und wie wird es genutzt?**	PIV (Personal Identity Verification) ist eine smartcardbasierte Anmeldeinformation, die vor allem von US-Bundesbehörden eingesetzt wird. Sie unterstützt zertifikatsbasierte Authentifizierung, digitale Signaturen und Verschlüsselung für den physischen wie den logischen Zugang.
F43 **Wie melde ich mich mit meinem PIV-Schlüssel an?**	Stecken Sie Ihren PIV-fähigen Schlüssel in ein Lesegerät und geben Sie bei Aufforderung Ihre PIV-PIN ein. Die Modelle SecureKey und SecurePass unterstützen PIV.
F44 **Wie ändere ich PIN, PUK oder Management-Schlüssel?**	Mit dem Hirsch uTrust Key Manager (Modelle SecureKey und SecurePass) oder mit der PIV-Verwaltungssoftware Ihrer Organisation.
F45 **Wie viele Fehlversuche sind bei PIN und PUK erlaubt, und was passiert bei einer Sperre?**	Sie haben jeweils 6 Versuche für PIN und PUK. Zu viele falsche PIN-Eingaben sperren die PIV-Anwendung, bis sie mit der PUK entsperrt wird. Nach zu vielen falschen PUK-Eingaben ist eine Neuausgabe über Ihre Ausweisstelle erforderlich.
F46 **Was tun, wenn mein PIV-Zertifikat abgelaufen ist?**	Wenden Sie sich an Ihre ausgebende Stelle oder Ihren Lifecycle-Arbeitsplatz, um das Zertifikat zu erneuern oder neu auszustellen.
F47 **Mein PIV-Schlüssel bzw. meine PIV-Karte wird nicht erkannt – was tun?**	Stecken Sie ihn bzw. sie erneut ein und prüfen Sie die Ausrichtung, probieren Sie ein anderes Lesegerät und stellen Sie sicher, dass unter Windows PIV-Treiber bzw. -Middleware installiert sind. Besteht das Problem weiterhin, wenden Sie sich an Ihre ausgebende Stelle oder den IT-Helpdesk.

F48 **Was bedeuten die Meldungen „Smartcard ist gesperrt“ oder „System kann Sie nicht anmelden“?**	„Smartcard ist gesperrt“ bedeutet, dass zu oft eine falsche PIN eingegeben wurde – lassen Sie die Karte bei Ihrer Ausweisstelle zurücksetzen. „System kann Sie nicht anmelden“ heißt meist, dass das System Ihr PIV-Zertifikat nicht validieren kann – wenden Sie sich an den IT-Support.
F49 **Was tun, wenn ich meinen PIV-Ausweis verliere?**	Melden Sie den Verlust sofort, damit Ihre Zugangsrechte und Zertifikate deaktiviert werden können. In der Regel erhalten Sie einen vorläufigen Ausweis.
F50 **Wie gehe ich mit einer neu ausgestellten PIV- oder CAC-Karte um?**	Starten Sie die erneute Registrierung über Ihr Serviceportal. Dabei müssen Sie Ihre Identität in der Regel mit einem Einmalcode oder per E-Mail bestätigen.
F51 **Unterstützt das uTrust Key Manager Tool das Laden von PIV-Zertifikaten?**	Derzeit nicht. Zum Testen des Ladens von PIV-Zertifikaten verwenden Sie den Hirsch uTrust Mini Driver.

08 OTP-AUTHENTIFIZIERUNG (HOTP)

F52 **Unterstützt mein SecureKey bzw. SecurePass Einmalpasswörter (OTP)?**	Ja. SecureKey und SecurePass unterstützen ab Werk HOTP (HMAC-based One-Time Password) und sind standardmäßig auf die Erzeugung 6-stelliger Codes eingestellt.
F53 **Wie programmiere ich meinen SecureKey bzw. SecurePass für OATH-HOTP?**	Gehen Sie im Hirsch uTrust Key Manager zu *Applications → OTP*, geben Sie Ihren geheimen OTP-Schlüssel ein und klicken Sie auf *Finish*. Danach erzeugt jede Berührung des Schlüssels einen neuen 6-stelligen Code.
F54 **Woher bekomme ich meinen HOTP-Seed bzw. geheimen Schlüssel?**	Der HOTP-Seed muss von dem Dienst stammen, der die HOTP-Authentifizierung bereitstellt – Sie können ihn nicht selbst erzeugen. Wenn Sie Ihren Schlüssel über Hirsch erworben haben, wenden Sie sich an unseren Vertrieb; wir können einen Seed bereitstellen.
F55 **Sollte ich HOTP oder TOTP verwenden?**	HOTP ist nicht auf Zeitsynchronisation angewiesen und daher zuverlässiger, z. B. bei SMS oder E-Mail mit unvorhersehbaren Verzögerungen. TOTP-Codes laufen dagegen nach einem festen Intervall ab (z. B. alle 30 Sekunden).
F56 **Gibt es bei HOTP Sicherheitsaspekte, die ich kennen sollte?**	Ein HOTP-Code läuft erst ab, wenn er verwendet wird; das Risiko bei Offenlegung ist daher etwas höher als bei TOTP. Verpasste Validierungen können zudem den Zähler zwischen Schlüssel und Server aus dem Takt bringen.

09 PGP-VERSCHLÜSSELUNG (SECUREKEY GOV ODER SECUREPASS)

F57 **Welches Gerät – SecureKey GOV oder SecurePass – unterstützt PGP?**	PGP wird vom SecureKey GOV unterstützt.
F58 **Was ist der Unterschied zwischen PGP und PIV beim SecureKey GOV?**	PGP dient der Verschlüsselung und Signatur von E-Mails, PIV in erster Linie der Authentifizierung.

F59 **Wie richte ich PGP auf meinem SecureKey GOV ein?**	Erzeugen Sie Ihr Schlüsselpaar mit GnuPG (bzw. GPG Suite unter macOS) und übertragen Sie anschließend die Unterschlüssel zur sicheren Aufbewahrung auf das OpenPGP-Applet Ihres GOV-Schlüssels.
F60 **Bietet Hirsch ein Tool zur Verwaltung von PGP-Schlüsseln an?**	Nein. Das Hirsch uTrust Key Manager Tool unterstützt nur FIDO, PIV und OTP. Für PGP verwenden Sie die GnuPG-Tools.
F61 **Ist es sicher, meinen privaten PGP-Schlüssel auf dem Gerät zu speichern?**	Ja. Der private Schlüssel wird im Secure Element erzeugt und gespeichert und verlässt es nie – er ist daher gegen Auslesen geschützt.
F62 **Was ist der Unterschied zwischen meinem öffentlichen und meinem privaten PGP-Schlüssel?**	Mit Ihrem öffentlichen Schlüssel werden Nachrichten verschlüsselt und Signaturen geprüft; mit Ihrem privaten Schlüssel entschlüsseln Sie Nachrichten und erstellen Signaturen.
F63 **Wie sichere ich meine PGP-Schlüssel?**	Erzeugen Sie den privaten Hauptschlüssel extern (nicht auf dem Gerät) und übertragen Sie nur die Unterschlüssel auf Ihren GOV-Schlüssel. So bleibt eine wiederherstellbare Sicherung erhalten.
F64 **Wie exportiere ich meinen öffentlichen PGP-Schlüssel?**	Exportieren Sie ihn mit Ihrem PGP-Tool oder E-Mail-Programm, damit Sie ihn mit anderen teilen können.
F65 **Wie widerrufe ich einen PGP-Schlüssel?**	Erzeugen Sie ein Widerrufszertifikat, veröffentlichen Sie es und informieren Sie alle, die Ihren öffentlichen Schlüssel besitzen, dass er nicht mehr gültig ist.
F66 **Wie viele Fehlversuche sind bei PGP-PIN und Admin-PIN erlaubt, und was passiert bei einer Sperre?**	Jeweils 3 Versuche. Ist die PIN gesperrt, können Sie nicht mehr signieren oder entschlüsseln, bis sie mit der Admin-PIN zurückgesetzt wird.
F67 **Wie konfiguriere ich PGP unter macOS oder Linux?**	Unter macOS verwenden Sie GPG Suite, unter Linux funktionieren die Standard-GnuPG-Tools. Eine Schritt-für-Schritt-Anleitung bietet der GPG-Leitfaden der Linux Foundation.

HIRSCH
Eisenstraße 2-4, Haus 3
65428 Rüsselsheim
+49 6142 4811950
@ info@hirschsecure.de
hirschsecure.com