



**Mehr Leistung als Standard**

**noris network**

## **Sichere Passwörter mit KeePassXC und Yubikey**

**Sebastian Claßen**

Senior IT Systems Engineer Agile Operations/Devops

Stand: Juni 2019



## Überblick

- **Warum Passwort-Manager?**
- **KeePass(XC)**
  - Einführung
  - Funktionen
- **Yubikey**
  - Einführung
  - Funktionen
- **Konfiguration**
  - Yubikey
  - KeePassXC
  - KeePass2Android

## Warum Passwort-Manager?



- **viele Dienste -> viele Passwörter**
  - wenige/ein Standard-Passwort
  - einfach zu merken -> Wörterbuch
- **Risiken**
  - Ausspähen bei Eingabe
  - Angriffe auf oder Leaks bei einem der Services
  - Habe ich alle Passwörter geändert?
- **Lösung: Passwort Manager**

## KeePass(XC)



- **OpenSource Passwort-Manager**
- **Implementierungen für unterschiedliche Plattformen**
  - Windows, Linux, Mac, Android
  - Datenbanken kompatibel (mit Einschränkungen)
- **Schutz der Datenbank**
  - Hauptschlüssel
  - Passwort, Schlüssel-Datei, Security-Token

## KeePass(XC) — Funktionen



- Verwaltung von Zugangsdaten
- Speicherung weiteren sensiblen Informationen
- Passwörter via Zwischenablage, Auto-Type, Plugins
- Kennwort-Generator
- teilweise Unterstützung für Cloud-Dienste
  
- **KeepassXC-Browser**
  - für Chrome/Chromium und Firefox
  - Zuordnung zu Web-Seiten in Datenbank gespeichert
  - <https://keepassxc.org/docs/keepassxc-browser-migration/>

## Yubikey



- **Hardware Security-Token der Firma Yubico**
  - aktuell Version 5
- **verschiedene Modelle**
  - USB-A, USB-C, NFC
- **2 Key-Slots**
- **Preis: ca. 50 €**

## Yubikey — Funktionen



- statisches Passwort
- Yubico OTP
- OATH HOTP (standardisiertes Verfahren)
- Challenge-Response HMAC-SHA1
- FIDO U2F (nur spezielle Versionen)
- SmartCard, z.B. für OpenPGP
  
- **Problem:**
  - Wie sichere ich mich gegen Verlust/Defekt des Tokens ab?

## Yubikey

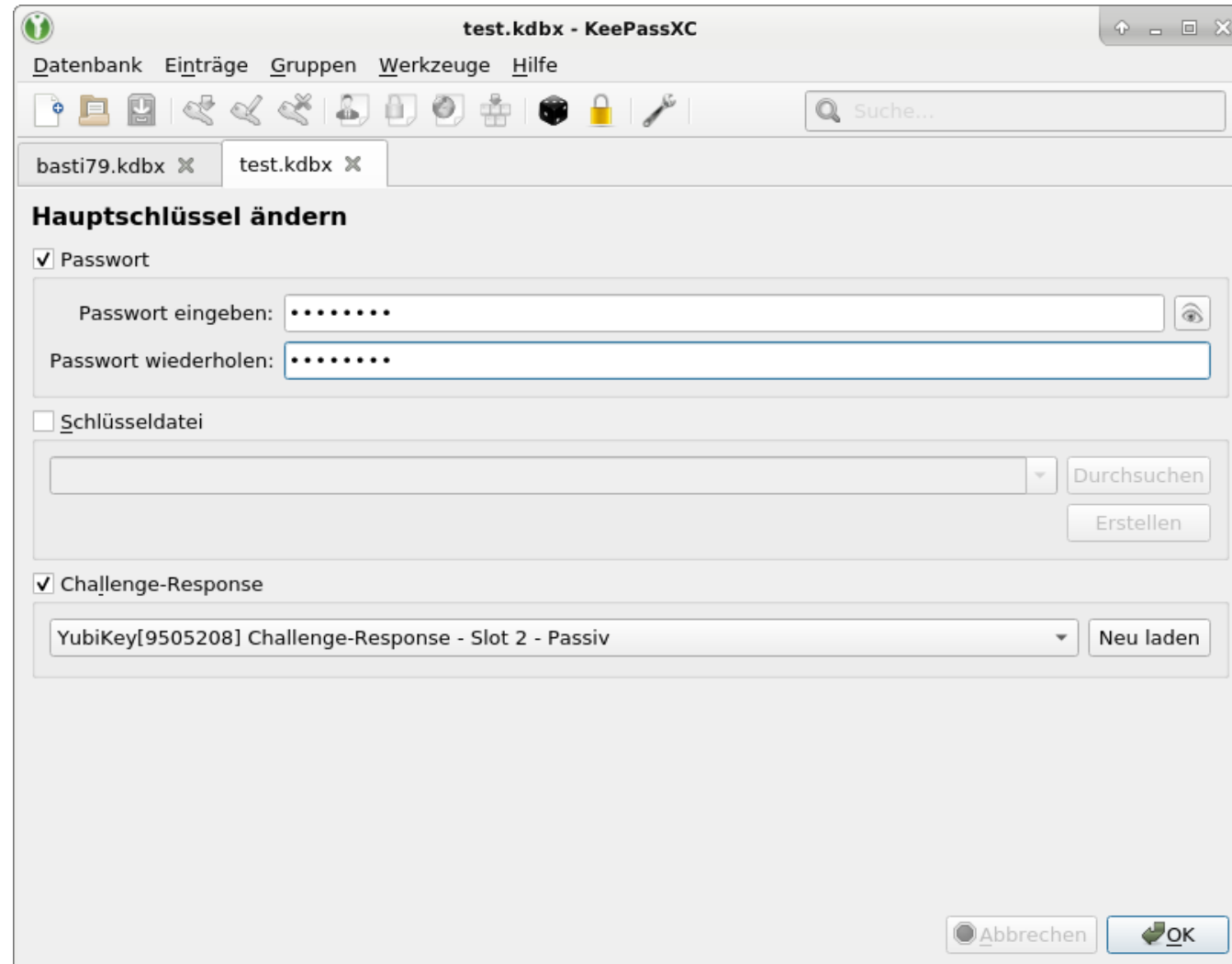
## Konfiguration

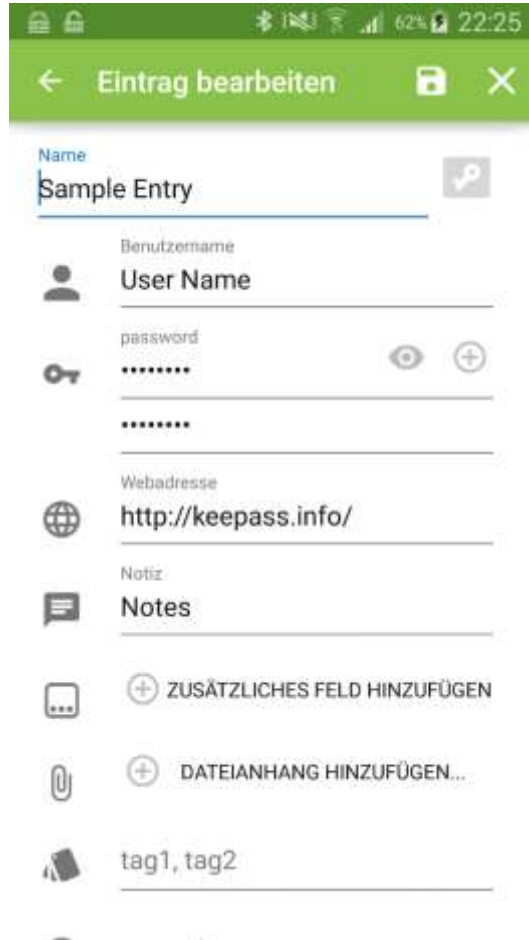
The screenshot shows the 'YubiKey Personalization Tool' window. The title bar includes a menu with 'Yubico OTP', 'OATH-HOTP', 'Static Password', 'Challenge-Response', 'Settings', 'Tools', 'About', and 'Exit'. The main content area is titled 'Program in Challenge-Response mode - HMAC-SHA1'. It contains several sections: 'Configuration Slot' with radio buttons for Slot 1 and Slot 2; 'Program Multiple YubiKeys' with a checkbox and a 'Randomize Secret' dropdown; 'Configuration Protection (6 bytes Hex)' with a dropdown menu and checkboxes for 'Use Serial Number' for current and new access codes; 'HMAC-SHA1 Parameters' with a 'Require user input' checkbox, 'Variable input' selected for the mode, and a 'Secret Key' field with a 'Generate' button; 'Actions' with 'Write Configuration', 'Stop', 'Reset', and 'Back' buttons; and 'Results' with a table header containing '#', 'Status', and 'Timestamp'. On the right side, there is a status panel with 'YubiKey is inserted', 'Programming status: Slot 1 and 2 configured', 'Firmware Version: 5.1.2', 'Serial Number' fields for Dec, Hex, and Modhex, and a 'Features Supported' list with checkmarks for Yubico OTP, 2 Configurations, OATH-HOTP, Static Password, Scan Code Mode, Challenge-Response, Updatable, Ndef, and Universal 2nd Factor. The Yubico logo is at the bottom right.



## KeepassXC

## Konfiguration





## Konfiguration — KeePass2Android

- **benötigte Apps:**
  - KeePass2Android Password Safe
  - ykDroid
- **Master Key Type:**
  - “Password + Challenge-Response for KeePassXC”
- **Problem: Synchronisation?**



Mehr Leistung als Standard

**noris** network

**Vielen Dank!  
Fragen?**

noris network AG  
Thomas-Mann-Straße 16 – 20  
90471 Nürnberg

Niederlassung München:  
Klausnerstr. 30  
85609 Aschheim

Telefon: +49 911 9352-0  
[www.noris.de](http://www.noris.de)  
[www.datacenter.de](http://www.datacenter.de)

**IT Sicherheit**  
  Made in Germany