Freie und flexible Zweifaktorauthentisierung mit LinOTP

17.03.2012 – CLT2012

Cornelius Kölbel, Stand 15.03.2012/, Revision 1

Ansprechpartner

- Dipl.-Phys. Cornelius Kölbel, Leiter Produktmanagement
  cornelius.koelbel@lsexperts.de

- LSE Leading Security Experts GmbH
  Robert-Koch-Str. 9
  64331 Weiterstadt

- Tel.: 06151 / 9067 – 0
  Fax: 06151 / 9067 – 299
  http:// www.lsexperts.de

Identitäten und Authentifizierung

Wissen und Besitz

- 1968: Odyssee im Weltraum: HAL macht Stimmerkennung
- 1971: Diamantenfieber: James Bond macht Fingerabdrücke
- 1982: Bladerunner: Rick Deckard macht Retina-Scan
- 1982: Zorn des Khan: Captian Kirk macht Retina-Scan
- 1986: RSA macht SecureID(R)

- Smartcard, Token, Einmal-Passwörter, Biometrie, OTP

Hersteller und Algorithmen

- Viele verschiedene Hersteller
- Viele verschiedene Algorithmen
  - OATH/ HOTP, TOTP, OCRA
  - mOTP
  - AES
  - DES
  - DPW, md5
  - …








Algorithmen

- Zeit oder Ereignis → Zähler, counter, movingFactor
- Seed: geheimer Schlüssel

- Im Wesentlichen:
  - *OTPvalue = otpAlgorithm(Seed, movingFactor)*

Token Typen

- Soft-Token
- SMS-Token
- Preseeded Hardware-Token
- Seedbare Hardware-Token

Benutzer

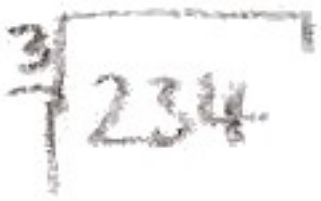
- LDAP

- SQL

- Flat file (wer was anderes kennt, bekommt kostenfrei eine 60-Tage Lizenz für 10 Token)

Mandanten

- Diensteanbieter
- Hosted Services
- Unternehmen (Abteilungen)
- Universitäten (Fachbereiche)



Workflow-Integration

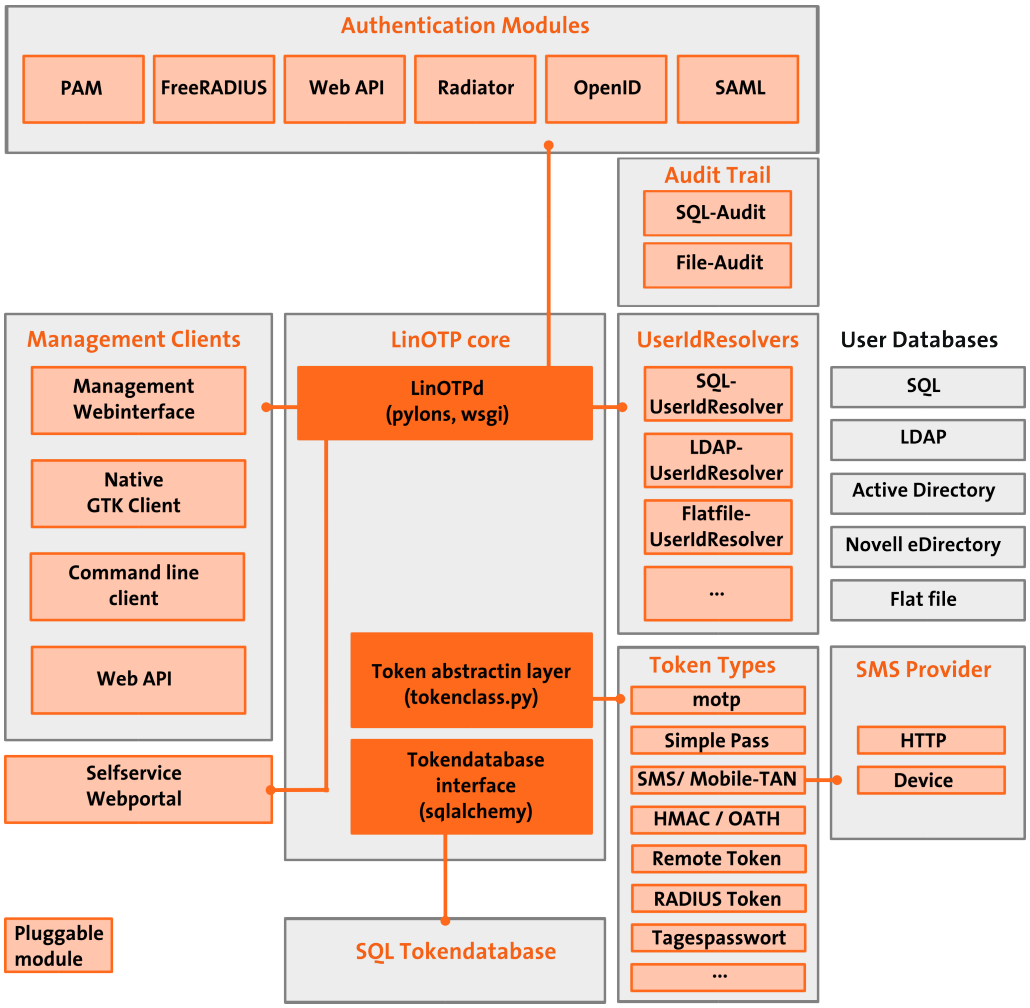
- Einbindung von Management-Funktione
  - Ausrollen von neuen Token
  - Sperren oder löschen von Token (HR)
  - PIN/Passwort Reset (Helpdesk)

- Einbindung von selfservice-Funktionen

- Authentisierung an verschiedensten Systemen

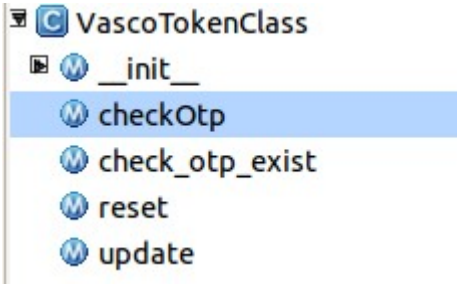
LinOTP: flexibel, modular

- Authentisierung
- Audit
- Benutzer
- Token
- Management und „Self-Management“
- Token-Datenbank

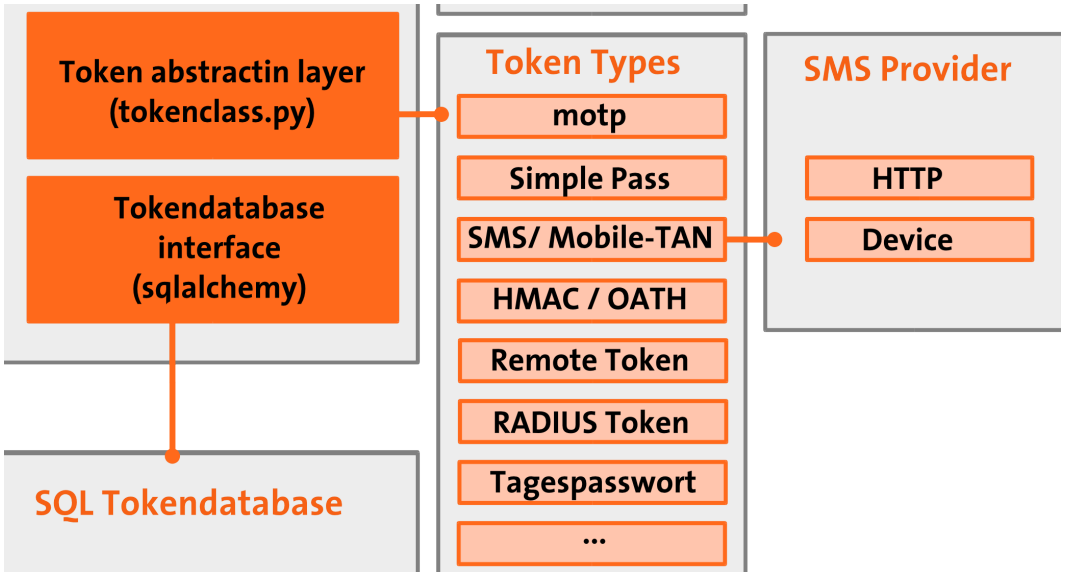


Hersteller und Algorithmen: Authentisierungs-Devices

- Abstraktion der Token-Funktion
  - → leichte Einbindung neuer Tokentypen
  - (vasco noch nicht aufgeführt, 70 Zeilen Code!)

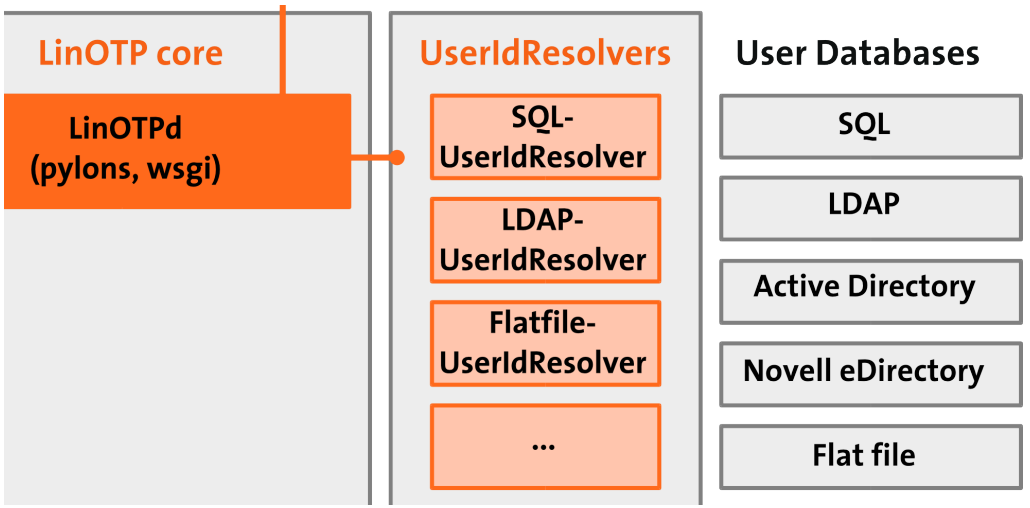


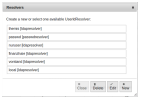
- SMS Token:
  - Abstraktion der SMS-Zustellung



Benutzer und Mandanten: UserIdResolver und Realms

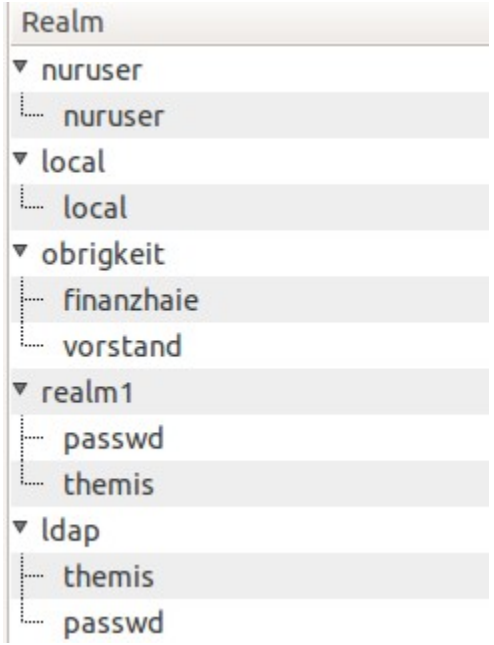
- Beliebige Anzahl an UserIdResolvern verschiedenster Art
- Stellen flexible Verbindung zu Benutzerquellen her
  - SQL: Spalten wählbar
    (sqlalchemy: MS SQL, Oracle, MySQL, PostgresQL....)
  - LDAP: Attribute map-bar
    (AD, OpenLDAP, eDirectory, Penrose virtual directory)

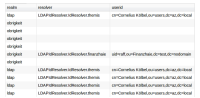




Benutzer und Mandanten: UserIdResolver und Realms

- Beliebige Bündelung der Resolver zu Realms
- Eindeutige Identifizierung eines Benutzerobjekts im System:
  - Realm
  - UserIdResolver (Klasse, Instanz)
  - UId





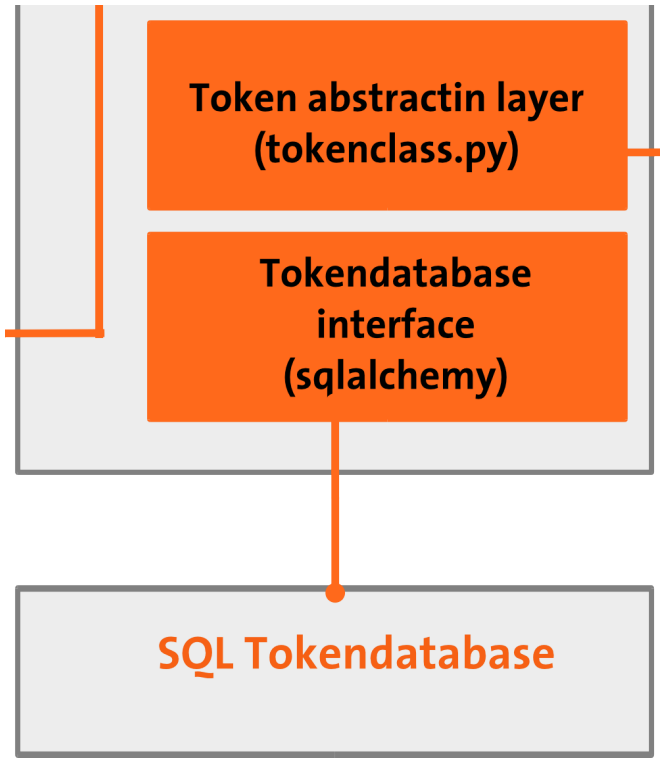
Benutzer und Token: Token-Datenbank

- Zuordnung der Token in der Token-Datenbank zum Benutzerobjekt (Realm, UserIdResolver, UId)

serial number	type	realm	resolver	userid
1000133508112	HMAC	ldap	LDAPIdResolver.IdResolver.themis	cn=Cornelius Kölbel,ou=users,dc=az,dc=local
AA000001	HMAC	obrigkeit		
AA000002	HMAC	obrigkeit		
AA000003	HMAC	obrigkeit		
AA000004	HMAC	obrigkeit		
AA000005	HMAC	obrigkeit	LDAPIdResolver.IdResolver.finanzhaie	uid=raff,ou=Finanzhaie,dc=test,dc=nodomain
AA000006	HMAC	obrigkeit		
LSGO12020914	HMAC	ldap	LDAPIdResolver.IdResolver.themis	cn=Cornelius Kölbel,ou=users,dc=az,dc=local
LSSM48964	sms	ldap	LDAPIdResolver.IdResolver.themis	cn=Cornelius Kölbel,ou=users,dc=az,dc=local
LSSM538C9	sms	ldap	LDAPIdResolver.IdResolver.themis	cn=Cornelius Kölbel,ou=users,dc=az,dc=local
oath4B380	HMAC	ldap	LDAPIdResolver.IdResolver.themis	cn=Cornelius Kölbel,ou=users,dc=az,dc=local
oath575A9	HMAC	ldap	LDAPIdResolver.IdResolver.themis	cn=Cornelius Kölbel,ou=users,dc=az,dc=local
oath6FBA3	HMAC	nuruser	LDAPIdResolver.IdResolver.nuruser	cn=user1,ou=users,dc=test,dc=nodomain

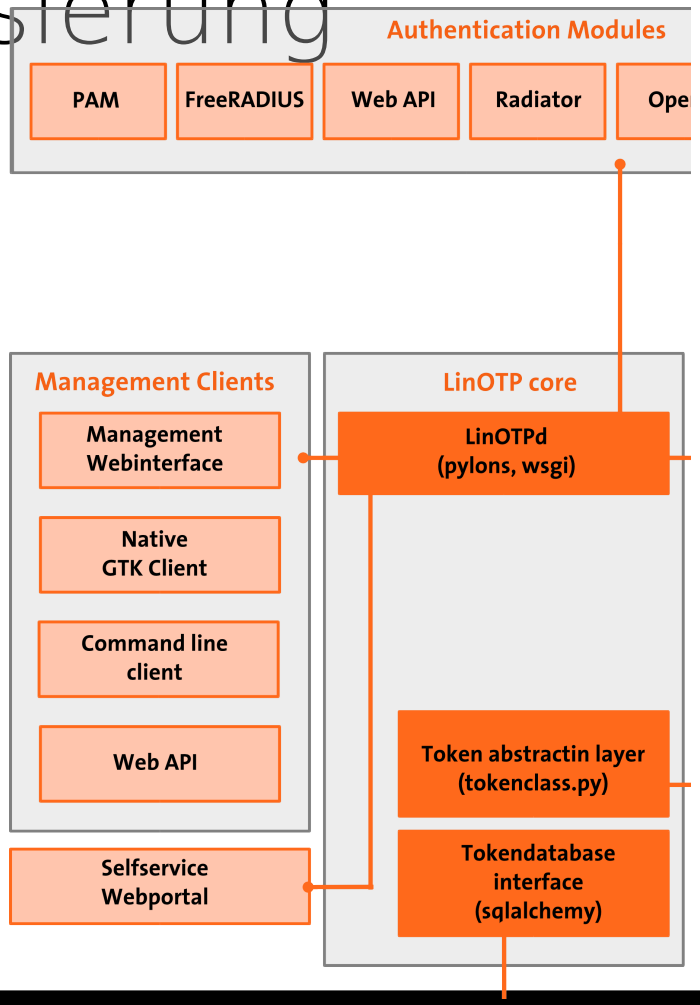
Benutzer und Token: Token-Datenbank

- SQL Alchemy
- Redundanz



Workflow-Integration API für Management und Authentisierung

- API für Management, Selfservice und Authentisierung



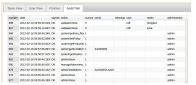
Workflow-Integration API für Management und Authentisierung

- → Einbindung in bestehende Applikationen

- → Management-Zugriffe steuerbar durch Rechte-Konzept und Policy-Definitionen
  - → Mandantenfähigkeit

PCI-DSS – Audit Trail

- Tracken von
  - Management-Aktivitäten
  - Benutzer-Aktivitäten
  - Benutzer-Authentisierungen
- Modularität (File, SQL, …)
- API erlaubt Signatur-Prüfung und Lösch-Identifizierung



LinOTP: flexibel, modular, offen

- Flexibler Austausch von Token-Datenbank und Audit-Modul
- Hinzufügen von Token-Typen
- Hinzufügen von Benutzer-Quell-Anbindungen
- Einbindung von Management-Funktionalitäten (Management API)
- Anbindung an Applikationen und Dienste (Authentisierungs API)

- AGPLv3 Kern
- auditierbar

Ausblick

- Appliance März 2012
- Flexibles Konzept gibt es her:
  - 2012: Smartcard/Zertifikats-Unterstützung und Anbindung von PKI-Komponenten

Hands on

- LDAP-Resolver:
  - Verschiedene Quellen
    „nuruser“, „local“ und „obrigkeit“
- SMS OTP:
  - Trigger mittels PIN-auth
- Tokeninfo:
  - max_auth_success
  - Siehe Lost-Token
- Autoassignment:
  - Enrollment einfach wie nie mit der „realm1“, user „raff“