

## Erfahrungsbericht über den Aufbau der PKI der

 **SWISS INTERBANK CLEARING**  
*A Telekurs Group Company*



**René G. Eberhard**  
Dipl. El.-Ing. HTL  
CEO

keyon  
Schönbodenstrasse 4  
8640 Rapperswil  
Switzerland

Tel +41 55 220 64 03  
Mobile +41 79 456 00 45  
Fax +41 55 220 64 01

www.keyon.ch eberhard@keyon.ch

# Agenda

keyon

- Über diesen Vortrag
- Vorstellung der Applikationen
- Anforderungen an die PKI
- Herausforderungen
- Phasen und Resultate der Umsetzung
- Unvorhergesehenes
- Schlussfolgerung

# Über diesen Vortrag

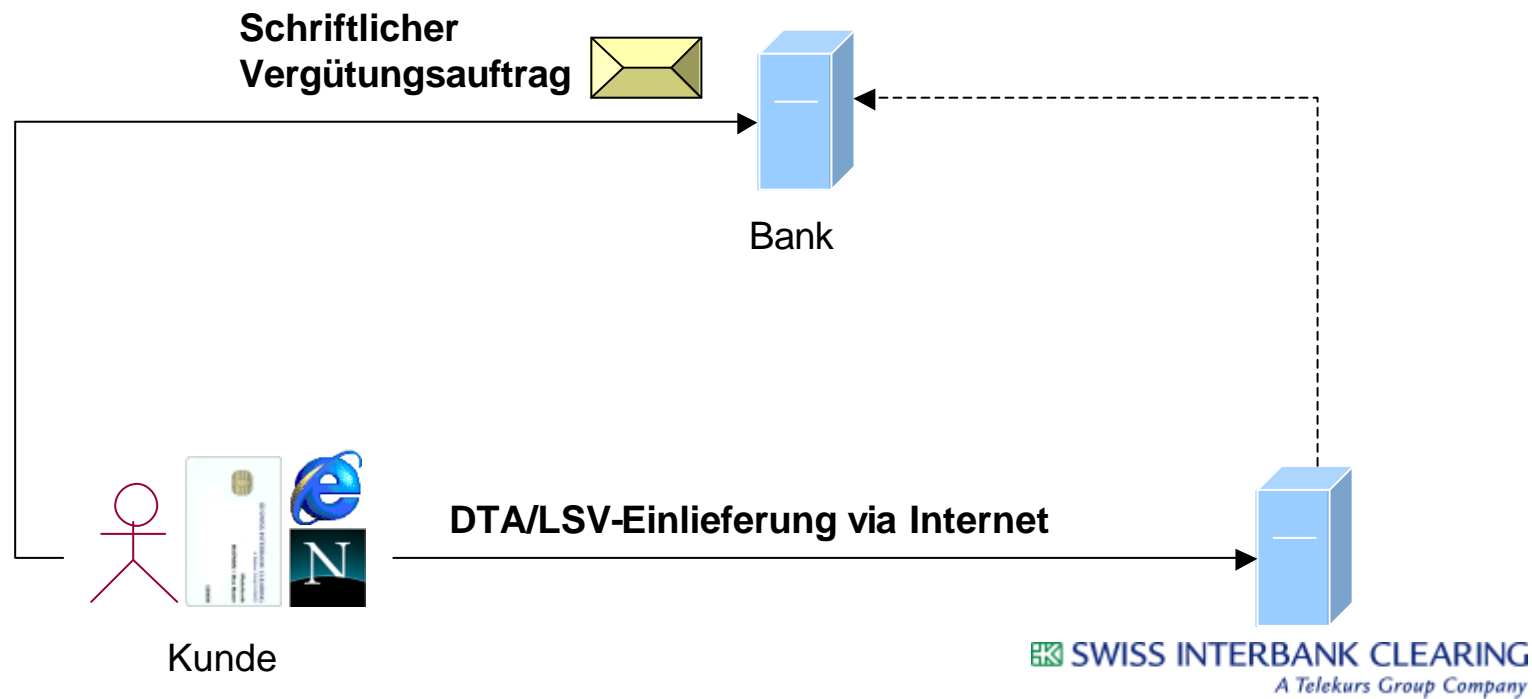
keyon

- Vortrag aus Sicht der PKI
- Abgrenzung
  - Keine Produktwerbung
  - Keine Offenlegung vertraulicher Internals
  - Die CA der SIC AG ist keine öffentliche CA

Kontaktperson der SIC AG  
Herr Paul Sutter  
Senior Manager  
Head of Payment Systems Architecture  
Email: paul.sutter@sic.ch  
Phone: +41 1 279 43 93

# Vorstellung PayCom<sup>web</sup>

keyon



# Vorstellung PayCom<sup>web</sup>

keyon



Kunde

Telekurs Swiss Interbank Clearing - PayComWeb - Microsoft Internet Explorer

Adresse <https://gate.sic.ch/paycomweb/index.jsp>

**SWISS INTERBANK CLEARING**  
A Telekurs Group Company

Home Hilfe Disclaimer

- Aufträge senden
- Gesendete Aufträge
- Rückmeldungen
- Kontakte
- Abmelden

### Gesendete Aufträge

aktualisieren

Dateityp	Dateiname	Status	Grösse	Datum
	<a href="#">DTA-Oktober_25102001_182820.dta</a>	Success	3,3KB	25 Oct 2001 18:28:20
	<a href="#">DTA-Oktober.dta</a>	Failure	3,3KB	25 Oct 2001 18:26:23
	<a href="#">DTA-September_28092001_153456.dta</a>	Success	3,6KB	28 Sep 2001 15:34:56

[PayCom<sup>web</sup>-Benutzeranleitung](#), pdf, 682 kb (Stand: August 2001)

Um dieses Dokument lesen, drucken oder auf Ihren PC speichern zu können, benötigen Sie den Adobe Acrobat Reader. Die aktuelle Version können Sie [kostenlos hier herunterladen](#).

- Français
- English

Internet

# Vorstellung PayGate<sup>web</sup>

keyon



# Vorstellung PayGate<sup>web</sup>

keyon

PayGate web

SWISS INTERBANK CLEARING  
A Telekurs Group Company

Home Drucken E-Mail an Support Disclaimer Info

- Aufträge
- Verträge
- Kontakte
- Abmelden

**Aufträge**

Aufträge anzeigen

Aktuelle Daten Abgeschl. Daten

Selektierte Aufträge bearbeiten

Ermächtigen Erm. aufheben Löschen

	DL	BC-Nr.	Auftr.	Zust.Code	Konto-Nummer	Vertrag	gew. Datum	Wwhrg	Betrag	Valid.	Status
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	104.231.056-8	nein	25.02.2002	CHF	7'234.40	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	110.101.061-4	ja	25.02.2002	CHF	230'412.65	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	110.110.054-7	nein	25.02.2002	CHF	501'232.45	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	120.171.061-3	ja	25.02.2002	CHF	3'015.30	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	160.401.061-2	nein	25.02.2002	CHF	127.95	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	170.181.761-4	?	25.02.2002	CHF	214'643.85	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	210.101.061-5	nein	25.02.2002	EUR	33'902.35	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	220.301.065-3	nein	25.02.2002	EUR	123'987.40	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	250.171.067-7	nein	25.02.2002	CHF	86'342.50	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	260.191.065-5	nein	25.02.2002	EUR	9'532.70	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	310.101.062-5	?	25.02.2002	CHF	13'902.65	OK	offen
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	310.171.061-5	nein	25.02.2002	CHF	412'532.90	NOK2	fehlerhaft
<input type="checkbox"/>	DTA	88884	TPSV4	produktiv	402.212.164-2	nein	25.02.2002	CHF	15'212.26	OK	offen

aktuelle Daten 30/30

**Auftrag**

BC-Nr.	88884	ursprüng. BC-Nr.	88884	Konto-Nr.	104.231.056-8
DL	DTA	Zustandscode	produktiv	Vertrag	nein
DTA/LSV-ID	TPSV4	Erstelldatum	25.02.2002	vorauss. Lauf	1
Gew. Verarb.datum	25.02.2002	Ausführungsbetrag	7'234.40	vor. Verrech.datum	27.02.2002
Währung	CHF			Mandatsspesen	0.00
Ermächt.betrag	7'234.40				

**Verrechnung**

Lauf 0

Benutzeranleitung



Bank

# Anforderungen

- *State of the art* Sicherheit
  - Sichere Übertragung der Daten (SSL)
  - Sichere Authentifizierung der Teilnehmer (Smart Card basierte Zertifikate)
- Business Case
  - Umsetzen der Geschäftsprozesse
  - Sicherstellen eines kostengünstigen Betriebs
  - Kommunikation zum Kunden
- Rechtliches
- Marketing
- Kostenkontrolle
- Projekt Management
- Integration
- Sicherheitskonzepte

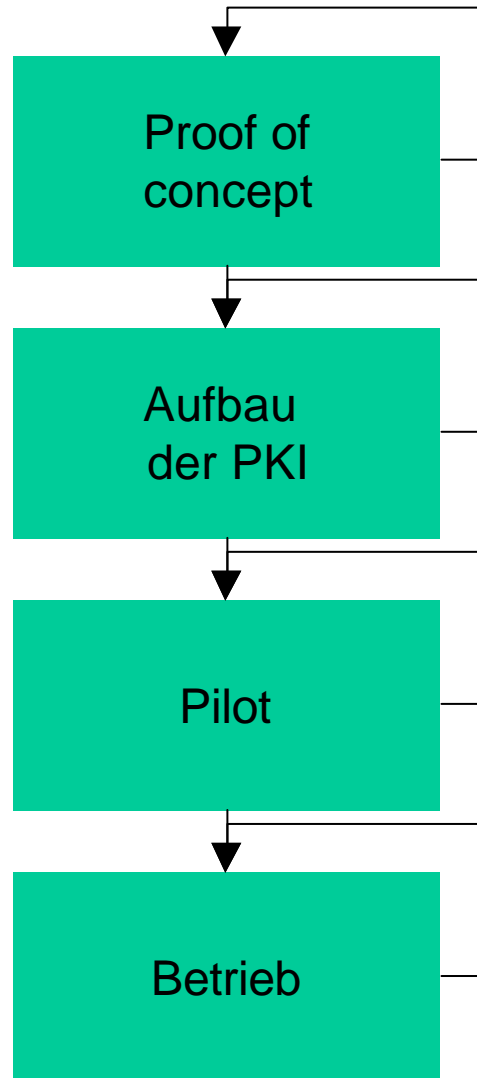


# Herausforderungen

- Ausgabe von Zertifikaten und Zertifikats Management
  - Swisskey hat Dienstleistung eingestellt
- Umsetzen der hohen Sicherheitsanforderungen
  - Implementation der Smart Card basierten Applikationen
  - Smart Card Management
  - Integration der Applikationen in bestehende Infrastruktur
  - Prozesse
  - Betrieb

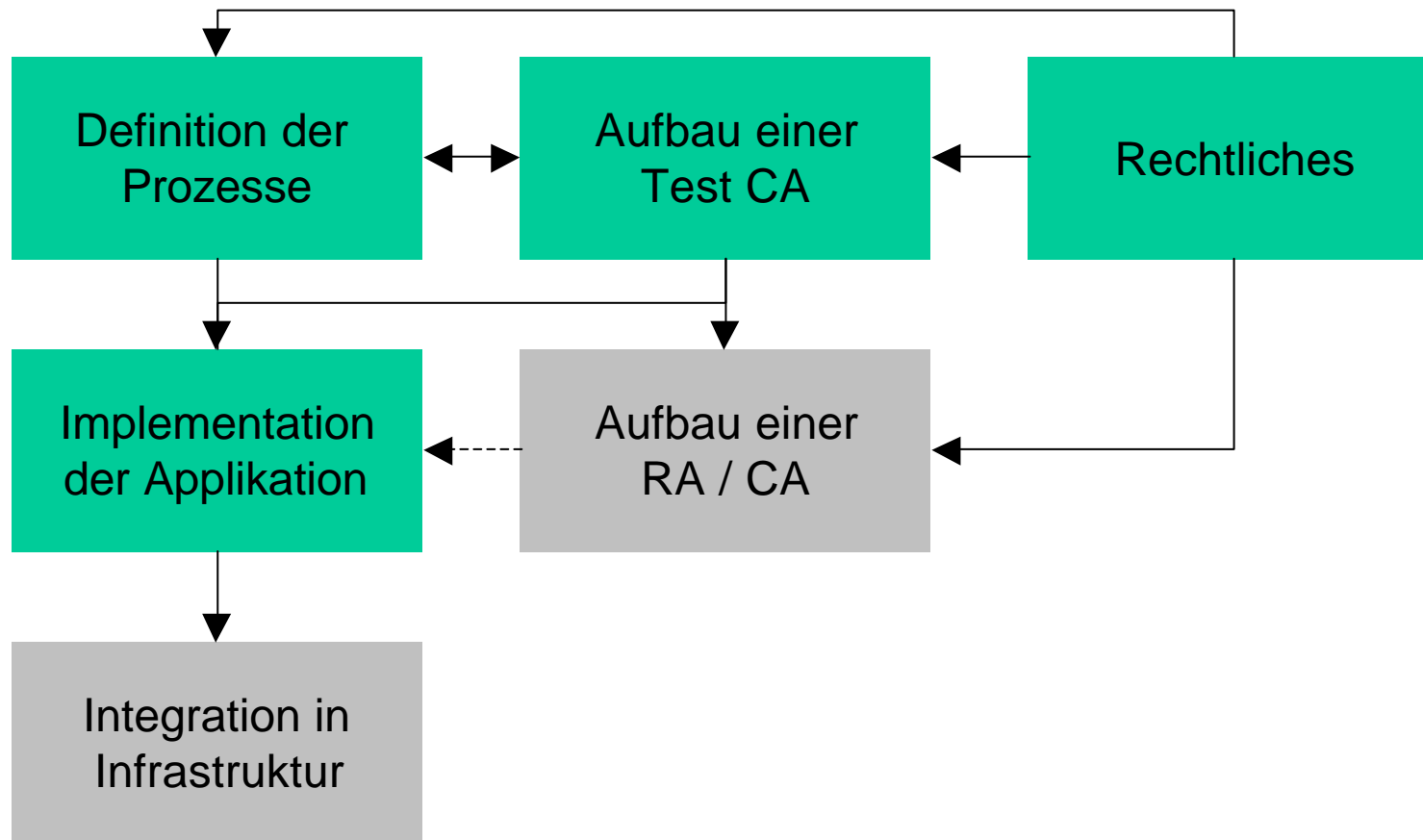
# Übersicht über die Phasen

keyon



# Phase 1 – Proof of concept

keyon



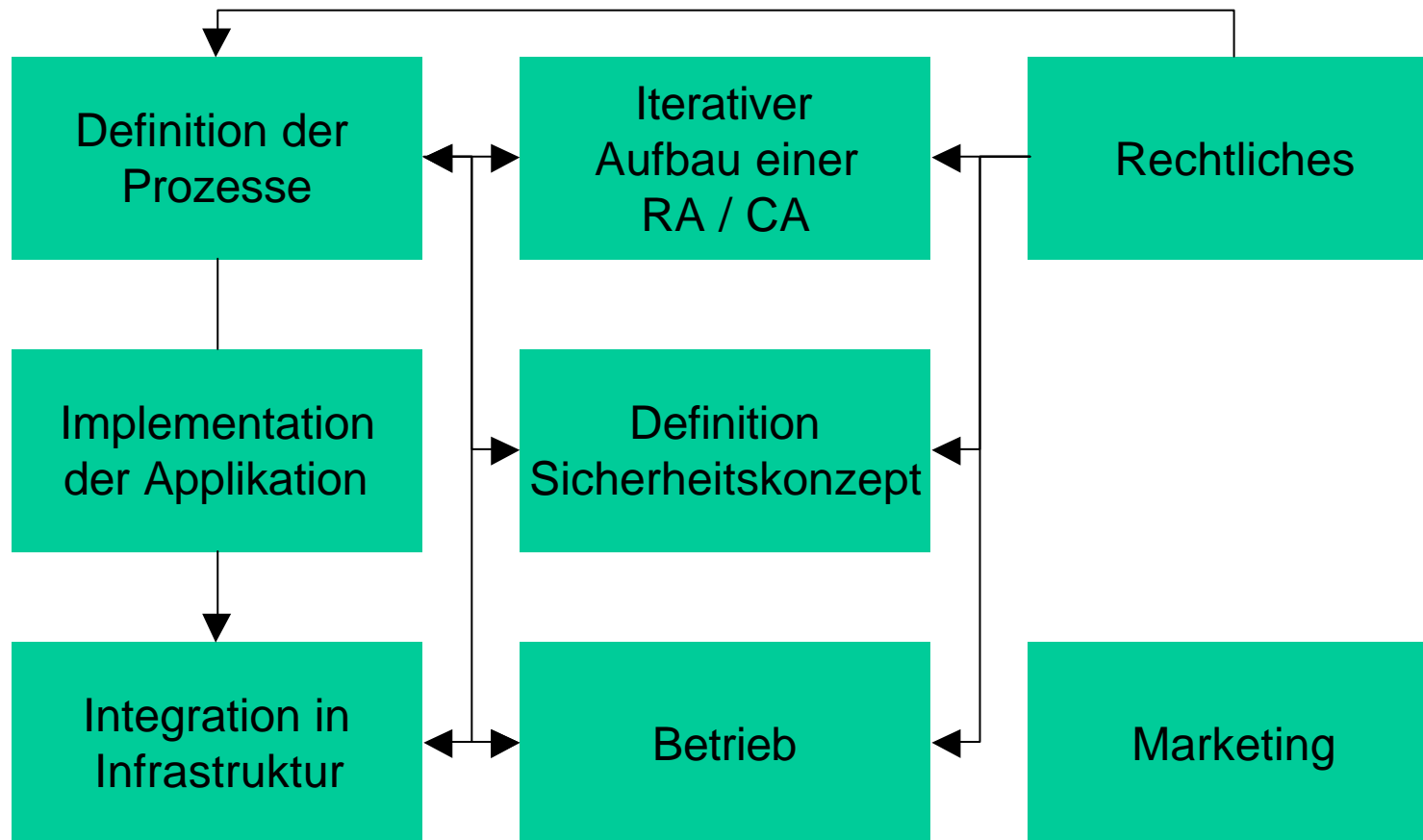
# Resultate der Phase 1

- Ausgabe von Test Zertifikaten auf Smart Card hat man unter Kontrolle
- Entwicklung von Applikationen kann parallel zu weiteren Phasen laufen
- Erste Iteration der Prozessdefinition
  - Möglichkeiten einer PKI aufgezeigt und verstanden
  - Erste Abbildung einer PKI auf Anwendungsfälle
    - Registrieren von Kunden
    - Nutzen von Zertifikaten in Applikationen

# Resultate der Phase 1

- Anforderungen an RA / CA
  - CA Software
  - CA Prozesse / Betrieb
  - Rechtliche Aspekte

# Phase 2 – Aufbau der PKI

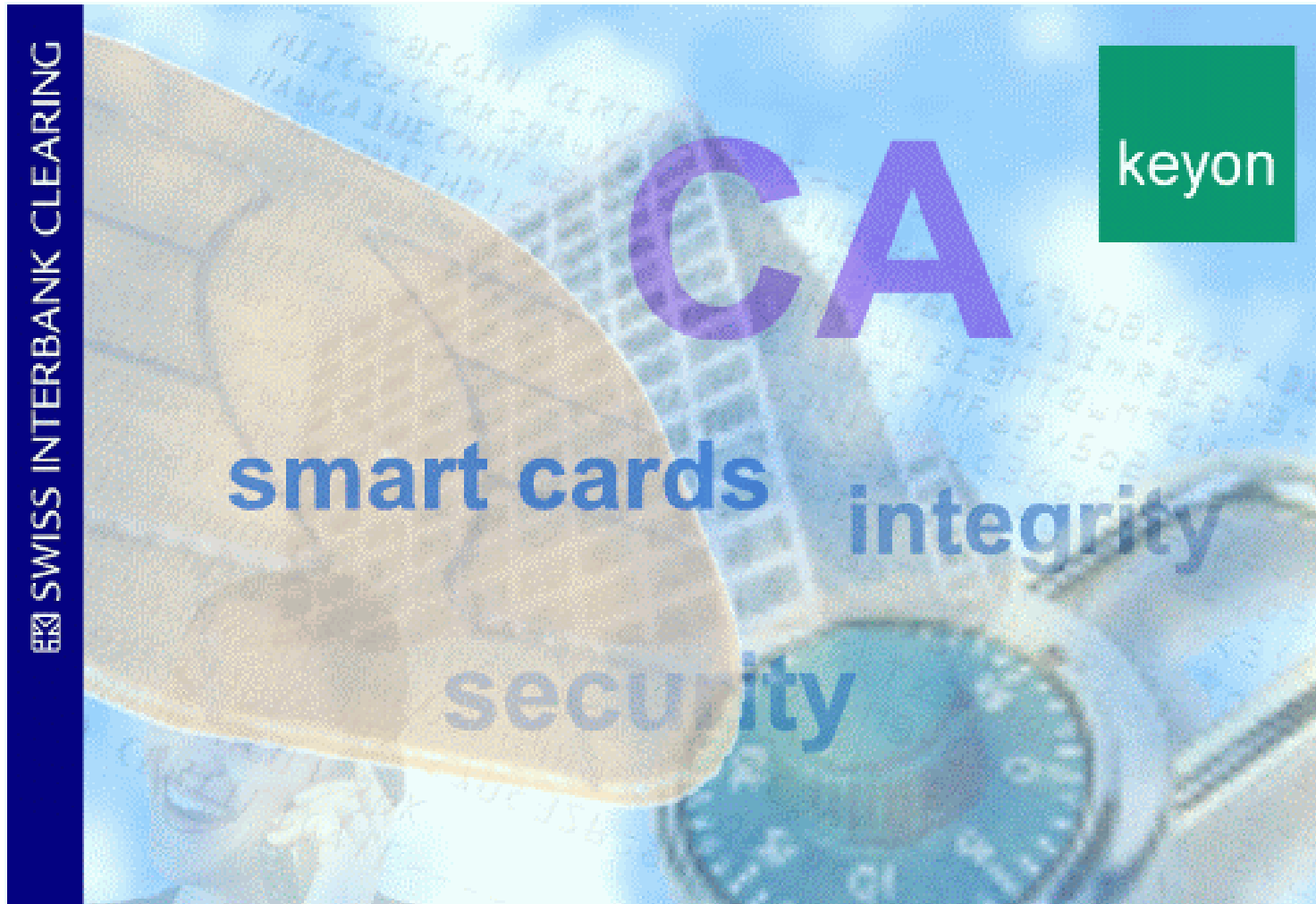


# Resultate der Phase 2

- SIC spezifische CA Software
  - Zertifikats und Smart Card Management
  - Prozesse und Administration auf SIC zugeschnitten
- Betrieb kann mit der CA Software Arbeiten
  - Iterative Entwicklung
    - Verstehen und *Leben* einer PKI
    - Einfluss auf Prozesse und Integration
  - Integration in Infrastruktur
    - Entry Server
    - Validation Server
    - Mapping Server
    - Change Management

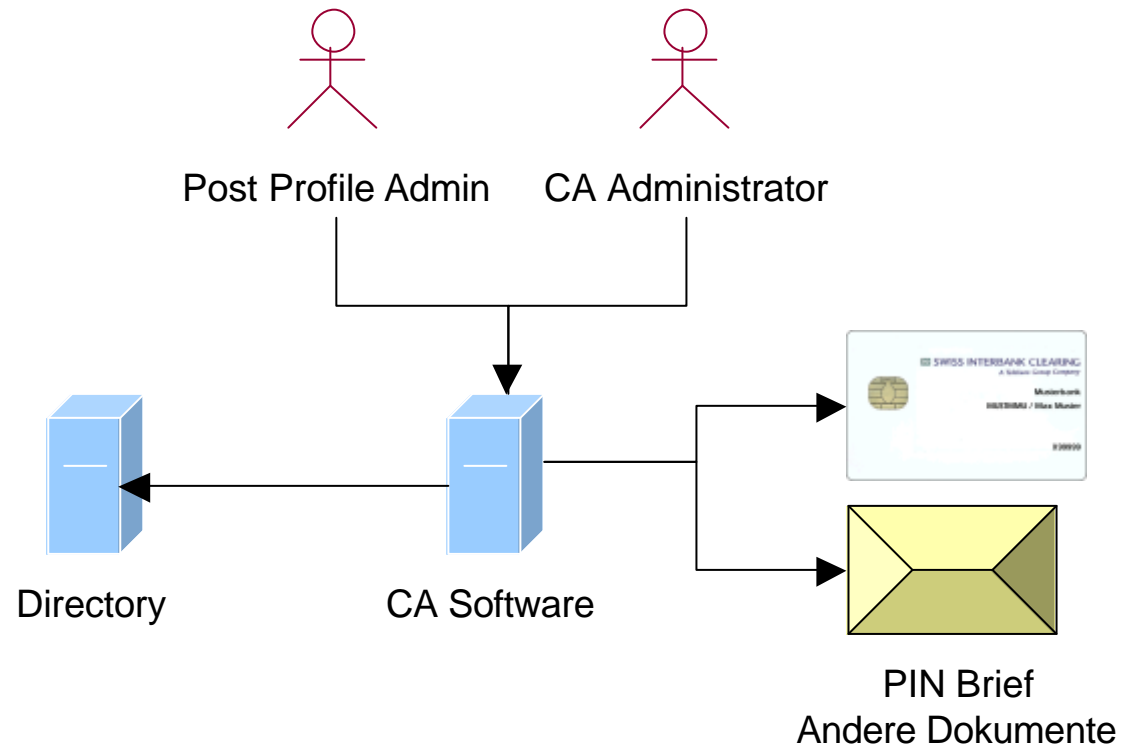
# Resultate der Phase 2 – CA Software

keyon





# Resultate der Phase 2 – CA Software



# Resultate der Phase 2 – CA Software

keyon

SIC CA - SIC CA 1024 Level 0

CA Database About

Issu DB Query Batch Import

Organization keyon Set as default

BPID X12345 Reset to default

Organizational Unit <sub>2</sub> Clear Form

Organizational Unit <sub>3</sub>

Country CH

State St. Gallen

Location Rapperswil

Common Name Rene Eberhard

E-Mail eberhard@keyon.ch Issue Token

Status: Logged in. 14. Mai. 2002 08:26

# Resultate der Phase 2 – CA Software

keyon

SIC CA Database - SIC CA 1024 Level 0

Generic query About to expire certificates CA certificates Revoked certificates

Query

Clear Query

View  
certificate   
token

Search criteria  
BPID contains   
OU<sub>2</sub> contains   
O contains   
CN contains   
EMAIL contains

Token issuing date  
 after 14.05.2002  
 until 14.05.2002  
Set today

Print

O	BPID	C	ST	L	CN	EMAIL	CERTS...	NOTBEF...	NOTAFT...	CERTIFI...	REVOK...	ISSUED	PASSW...
Payserv	ghmei	CH	Zuerich	Zuerich	gerhard ...	ghmei...	02	13.05.2...	13.05.2...	sh...		13.05.2...	s...
Payserv	petdoe	CH	Zuerich	Zuerich	peter do...	petdoe...	03	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	ulrgem	CH	Zuerich	Zuerich	ulrich g...	ulrgem...	04	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	retosw	CH	Zuerich	Zuerich	reto os...	retosw...	05	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	chrbok	CH	Zuerich	Zuerich	chris bo...	chrbok...	06	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	carbac	CH	Zuerich	Zuerich	carlo ba...	carbac...	07	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	sveber	CH	Zuerich	Zuerich	sven be...	sveber...	08	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	pauhub	CH	Zuerich	Zuerich	paul hu...	pauhub...	09	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...
Payserv	karmei	CH	Zuerich	Zuerich	karin m...	karmei...	0a	13.05.2...	13.05.2...	[X.509]		13.05.2...	[Passw...

CSV-Export Status: Query finished - 9 entrys found Close

# Resultate der Phase 2 – CA Software

**Initialize CA**

1. Define DN of the CA  
2. Define CA settings  
3. Define User Cert Settings  
4. Define PKCS#12 Settings  
5. Define V3 Extensions  
6. Define LDIF data  
7. User concept  
8. Define CA users  
9. Assign Role 1 Users  
10. Assign Role 2 Users  
11. Assign Role 3 Users  
12. Create CA

CA certificate extensions :

**Key usage :**  **KeyCertSign**  **CRLSign**

User certificate extensions :

**Key usage :**  **DigitalSignature**  **Extended**  **ClientAuthentication**  
 **NonRepudiation**  **EmailProtection**  
 **KeyEncipherment**  **CodeSigning**

**Certificate Policies OID :**

**URL :**

**CRL Distribution Point :**

**NS Revocation URL :**

**NS CA Policy URL :**

**NS Comment :**

< Back   Next >   Finish   Cancel

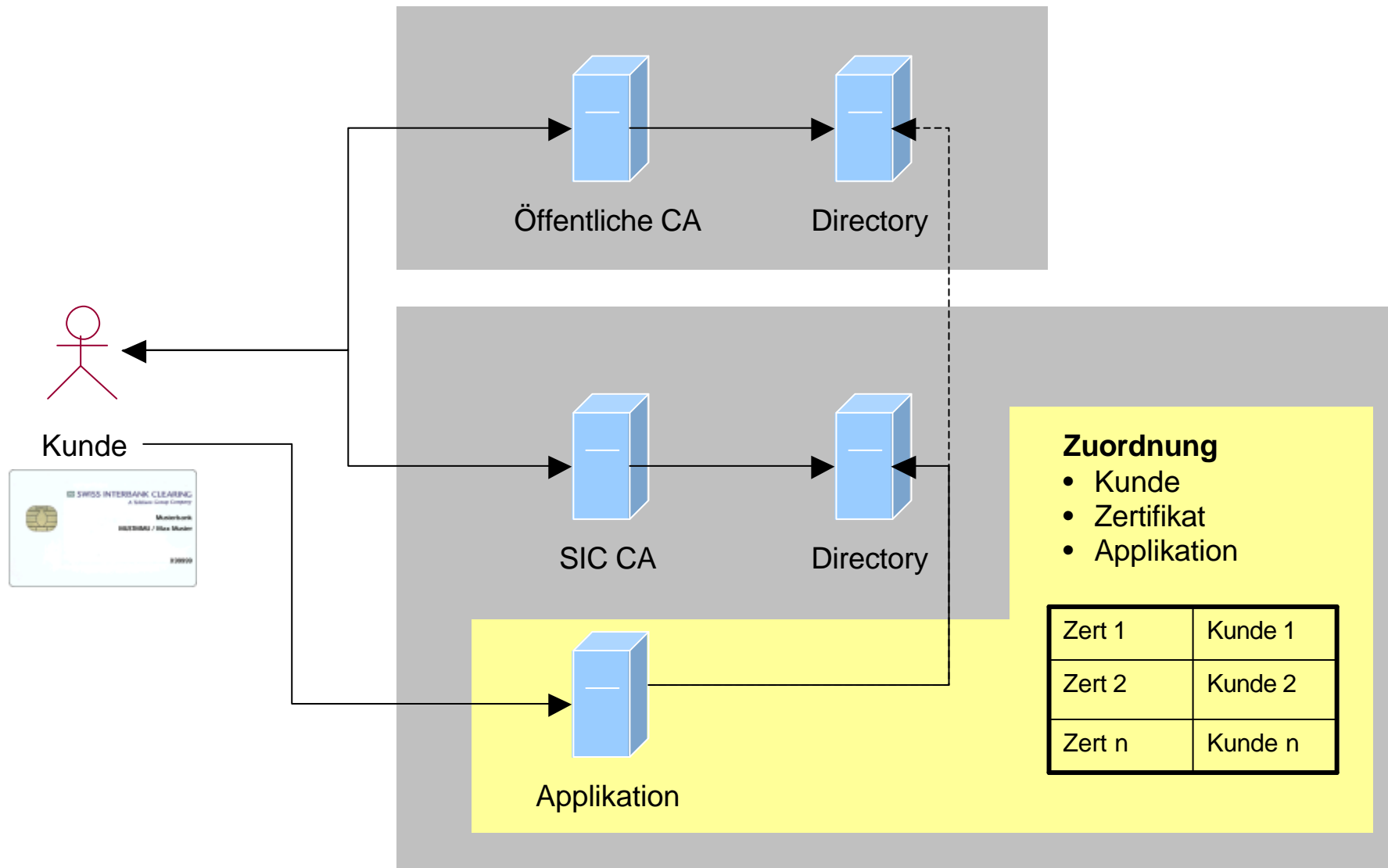
# Resultate der Phase 2

- Definition der Prozesse
  - Initialisieren der CA
  - Registrierung von Kunden
  - Ausgabe von Zertifikaten an Kunden
  - Sperren von Dienstleistungen und Zertifikaten
  - Mutationen von Daten
  - Zuordnen von Zertifikaten zu Applikationen
- Sicherheitskonzept
  - CA spezifisches Sicherheitskonzept
  - Applikationsspezifisches Sicherheitskonzept

# Resultate der Phase 2

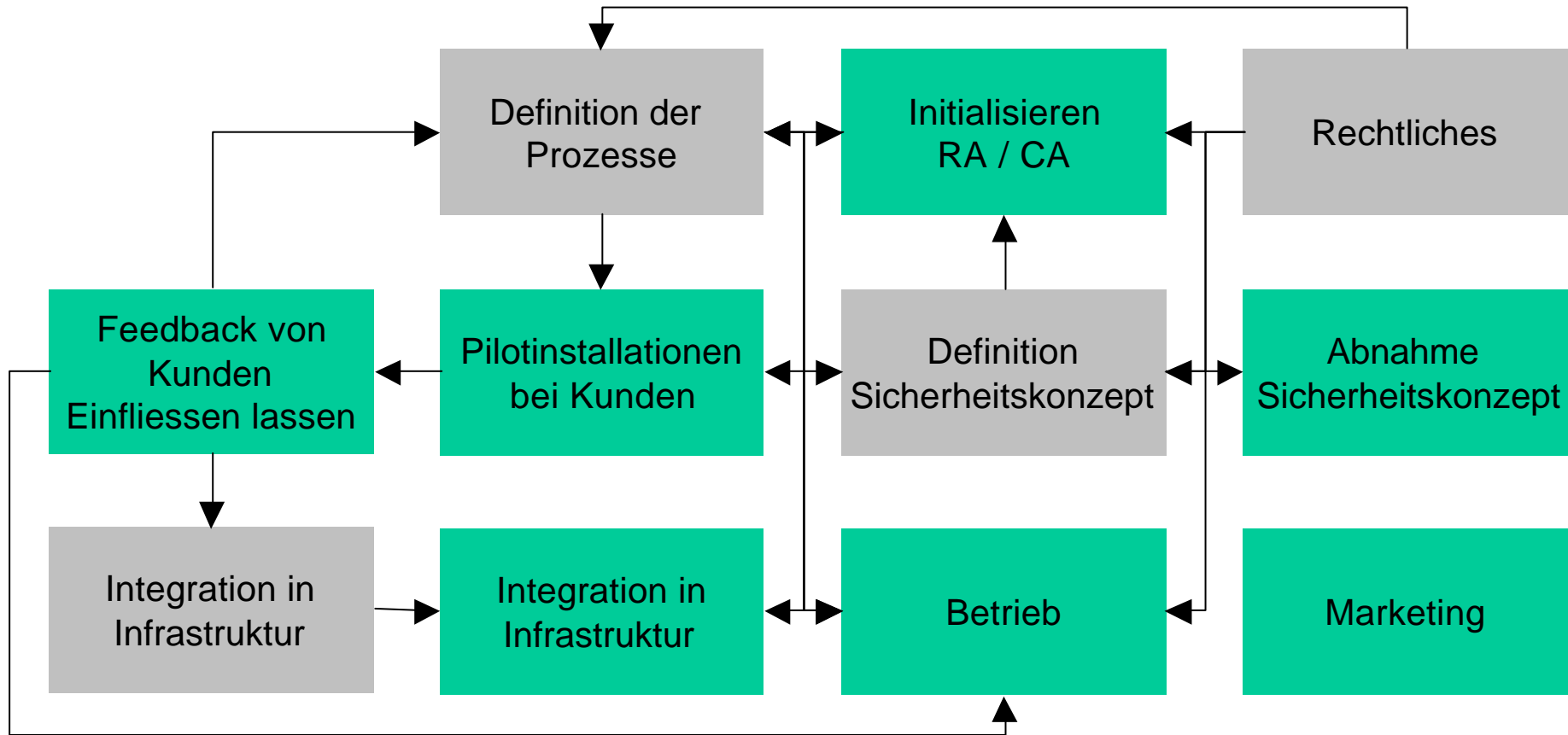
- Definition der CA Richtlinien
  - Abgrenzung und Verwendungszweck
  - Einsatz von Zertifikaten in Applikationen
- Rechtliches
  - Abbilden der rechtlichen Situation auf die PKI
  - Nutzungsbestimmungen und Disclaimer
  - Haftungsklauseln

# Resultate der Phase 2



# Phase 3 – Pilot

keyon





# Resultate der Phase 3

- CA Initialisiert
  - CA gemäss Sicherheitskonzept initialisiert
  - Administratoren, Zugriffskonzept und Archivierung definiert und geschult
- PKI in Infrastruktur integriert
  - Personal geschult
  - CA und Applikationen Einsatzbereit

# Resultate der Phase 3

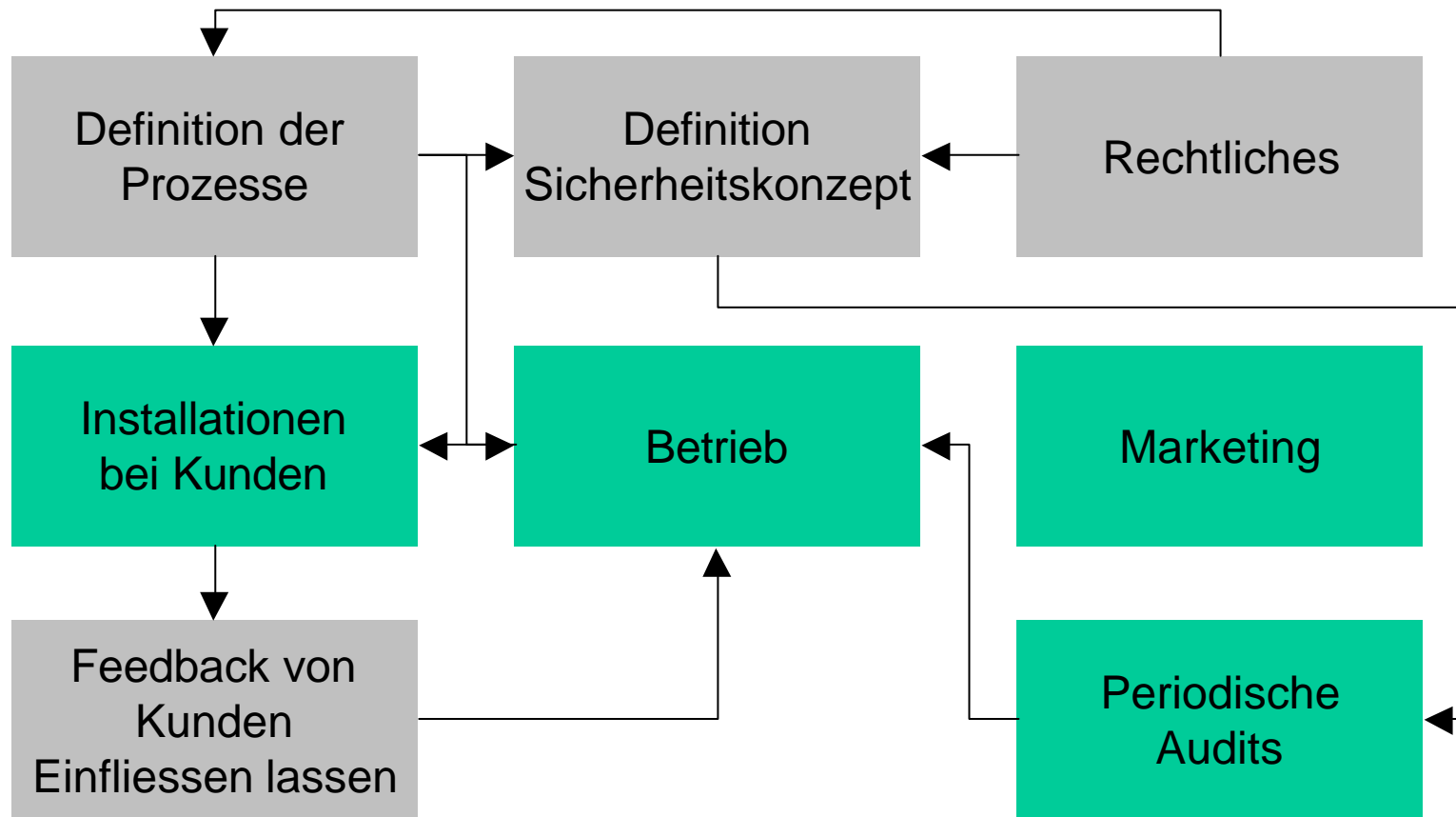
- Pilotinstallationen bei Kunden
  - Installationsanleitungen, Antragsformulare und Verträge sind bereit
  - Rollout der Zertifikate und Software erfolgt
  - Installation der Software beim Kunde
  - Feedback vom Kunden
  - Erfassen und beheben von Problemen
    - Unverständliche Formulare oder Anleitungen
    - Probleme bei der Installation oder Bedienung der Software
    - Probleme bei der Kommunikation über das Internet (Firewall, Proxy)

# Resultate der Phase 3

- Integration der PKI in Infrastruktur
  - Ausführliche Tests der Systeme
    - Ausgeben von Zertifikaten
    - Sperren von Zertifikaten oder Dienstleistungen
    - Performance Tests
    - Einrichten von Überwachungssystemen
    - Change Management

# Phase 4 – Produktiver Betrieb

keyon



# Unvorhergesehenes

keyon

- Änderungen von Produkteigenschaften
- Kundenspezifische Konfigurationen
  - Firewall, Proxy
  - Betriebssysteme und Rechte
  - Prozesse

# Schlussfolgerung

- Erfolgreiches Projekt
  - Alle Anforderungen wurden erfüllt
  - Produktiver Einsatz der Applikationen
  - Effizienter und sicherer Betrieb der Applikationen
  - Termine und Kosten wurden eingehalten
- Fokussieren auf das Wesentliche
  - PKI unterstützt Business Case
  - Einsatz von Zertifikaten abgrenzen und gem. Business Case und rechtlichen Rahmenbedingungen definieren

- Tatsächliche Herausforderungen
  - Beschreiben der Prozesse und Sicherheitskonzepte
    - Faktor Mensch
    - Berücksichtigen etablierter Prozesse
  - Berücksichtigen existierender Rahmenbedingungen
    - Betrieblichen Aspekte
    - Bestehende Applikationen und Infrastrukturen
  - Abbilden der rechtlichen Situation auf die PKI

Danke für Ihre Aufmerksamkeit

keyon



**Für allfällige Fragen stehe ich  
Ihnen gerne zur Verfügung**