# XignQR

## The **X** in Signatures

The Quick Response Authentication & Signature System

# Inhalt

- Team
- Aktuell Ansätze – Problem bisheriger Lösungen
- Produkt – Authentifizierung & Signaturen durch QR Codes
- Produkt – Handel & Commerce
- Produkt – Internet of the Things & M2M
- Kontakt
- Appendix

# Team

## 70 Jahre Erfahrung im Bereich IT-Sicherheit

- **Pascal Manaras**
  - Expertise in Wirtschaft und Identitymanagement
  - Langjährige Erfahrung im Bereich der Entwicklung von verteilten Systemen, Client-Server-Architekturen, Protokollen und digitalen Identitäten
  - Mehrjährige Erfahrung in der Entwicklung von mobile Anwendungen

- **Markus Hertlein**
  - Expertise im Bereich Kryptographie und Gestaltung
  - Langjährige Erfahrung im Bereich der Smartcardentwicklung, Public-Key-Infrastrukturen und Verschlüsselung
  - Mehrjähriges Mitwirken am Internet-Kennzahlen, -Analyse und Frühwarnsystem

# Team

## 70 Jahre Erfahrung im Bereich IT-Sicherheit

- **Prof. Dr. Nobert Pohlmann**
  - 28 Jahre Erfahrung als Gründer, Unternehmer, Geschäftsführer, und Vorstandsmitglied, z.B. der Kryptokom GmbH und Utimaco Safeware AG, so wie als Informatikprofessor und Institutsleiter des renomierten Instituts für Internet-Sicherheit – if(is)
  - hohe Vernetzung durch diverse Verbandstätigkeiten, z.B. als Vorstandsvorsitzender Bundesverband IT-Sicherheit – TeleTrusT oder als Vorstandsmitglied des eco Verband der Internetwirtschaft

# Team

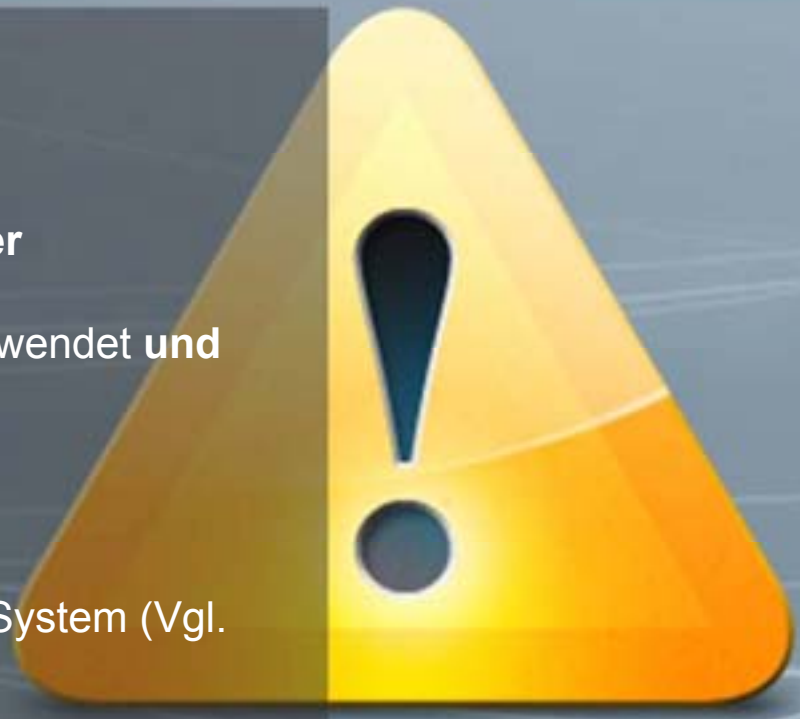
## 70 Jahre Erfahrung im Bereich IT-Sicherheit

- **Willi Mannheims**
  - 25 Jahre Erfahrung als Gründer, Unternehmer, Geschäftsführer von IT-Security Unternehmen, z.B. der Secunet AG, der Escrypt GmbH und exceed AG, mit erfolgreichen Börsengängen
  - 10 Jährige Private Equity- / Beteiligungs-Erfahrung mit Venture Capital Fond Daimler Chrysler, Vorndran Mannheims Capital GmbH, Mannheims Beteiligungsgesellschaft mbH
  - Weitreichendes Partnernetzwerk und Gespür für den Markt durch zahlreiche Vorstandsmitgliedschaften und Aufsichtsradmandate

# Aktuell Ansätze

## Probleme bisheriger Lösungen

- **Passwörter …**
  - … können einfach erraten werden **oder**
  - … können nur schwer im Kopf behalten werden **oder**
  - … werden häufig für mehr als ein Benutzerprofil verwendet **und**
  - … sind anfällig für eine Vielzahl von Angriffen
- **One-Time-Passwords / TANs**
  - Gestohlenes 'root secret' korrumpiert gesamtes System (Vgl. Lockheed Martin und RSA SecurID)
  - Die meisten Probleme von Passwörtern bleiben bestehen
- **Challenge Response**
  - Benötigt spezielle Hardware
  - Begrenzte Anzahl an Use Cases



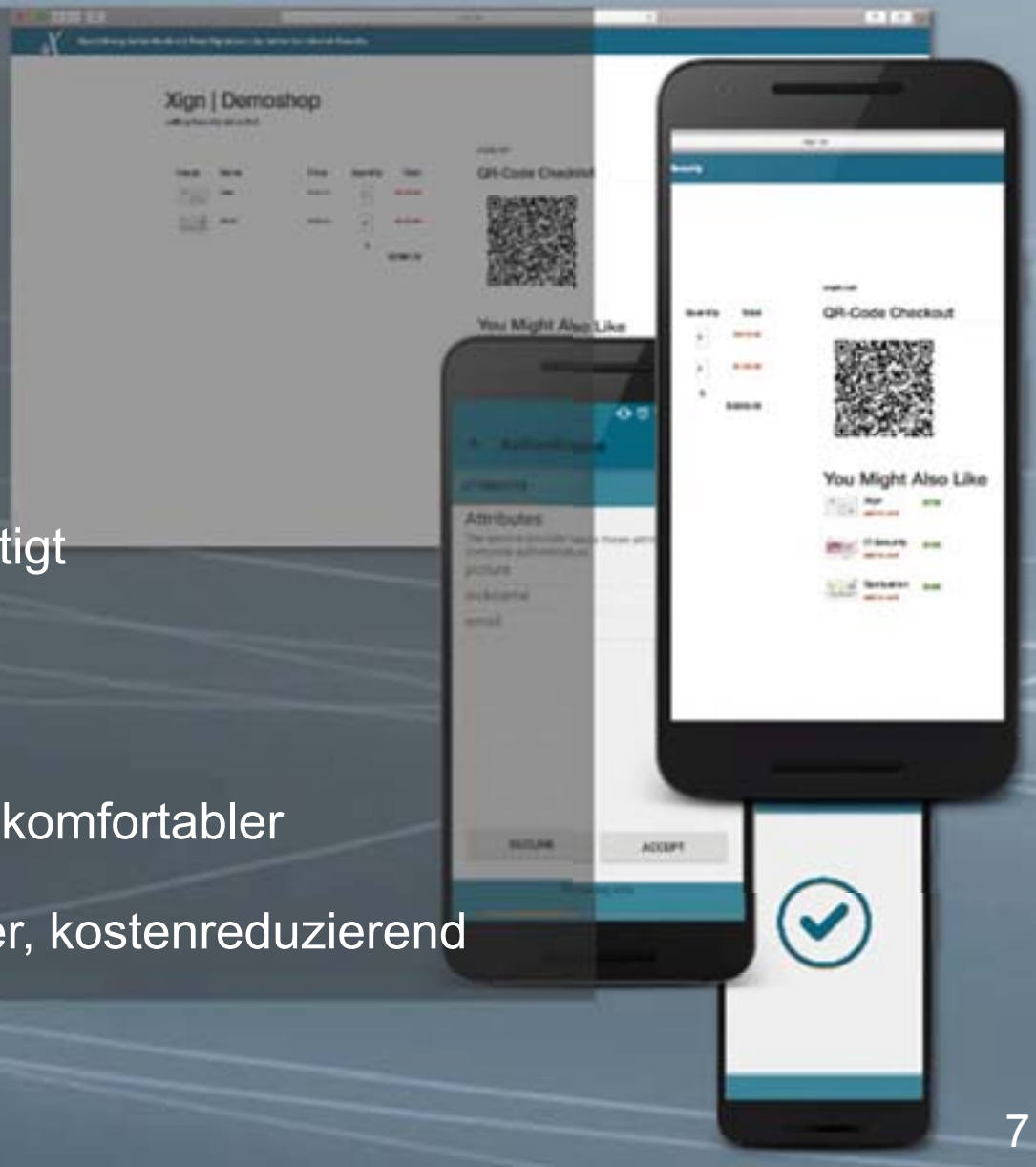
# Produkt

## Authentifizierung & Signaturen durch QR Codes

- 1. Nutzer bekommt QR Code präsentiert
  - Login / Shopping / Transaktionen / Signaturen
- 2. Nutzer scannt/fotografiert QR Code
- 3. Nutzer prüft Daten und bestätigt
- 4. Fertig!

→ Für Nutzer: Schneller, sicherer, komfortabler

→ Für Anbieter: Sicherer, wartbarer, kostenreduzierend



# Produkt

## Konzept

- QR Code als Einsprungspunkt
- Smartphone als persönliches Authentifizierungsdevice
- Gesteigerte Sicherheit durch Security Token (optional)
- Public-Key-Infrastruktur gestützt
- Passwortlose sichere Authentifizierung
- Nutzen und Einhalten von Standards wo es möglich ist
- Authentifizierung in unzähligen Szenarien
- Nutzererfahrung und Akzeptanz als Gut
- Verzicht auf zusätzliche Hardware wie Lesegeräte
- Sicherheit und Einfachheit bei allen Prozessen

# Produkt

## Merkmale

- **Eine Registrierung und Plattformunabhängigkeit**
  - Viele Anwendungen und Märkte in der realen und digitalen Welt mit riesigen Kundenklientel
- **Datenschutz und –sicherheit made in Germany**
  - Höchste Sicherheitsmerkmale und Datensparsamkeit
- **Nicht trackbar und die Möglichkeit zur Pseudonymität**
- **Einfache Integration, Wartbarkeit und Risikomanagement**
  - Reduzierte Komplexität
- **Geringe Interaktion → Einfach, schnell, benutzerfreundlich**
  - Keine Passwörter, nur scannen, bestätigen, fertig!
- **Hohe Nutzerakzeptanz und schnelle Verbreitung**
  - QR Code + Smartphone: kleiner Absprung, höher Conversions
- **Verwendung aus der Cloud oder on-premise**

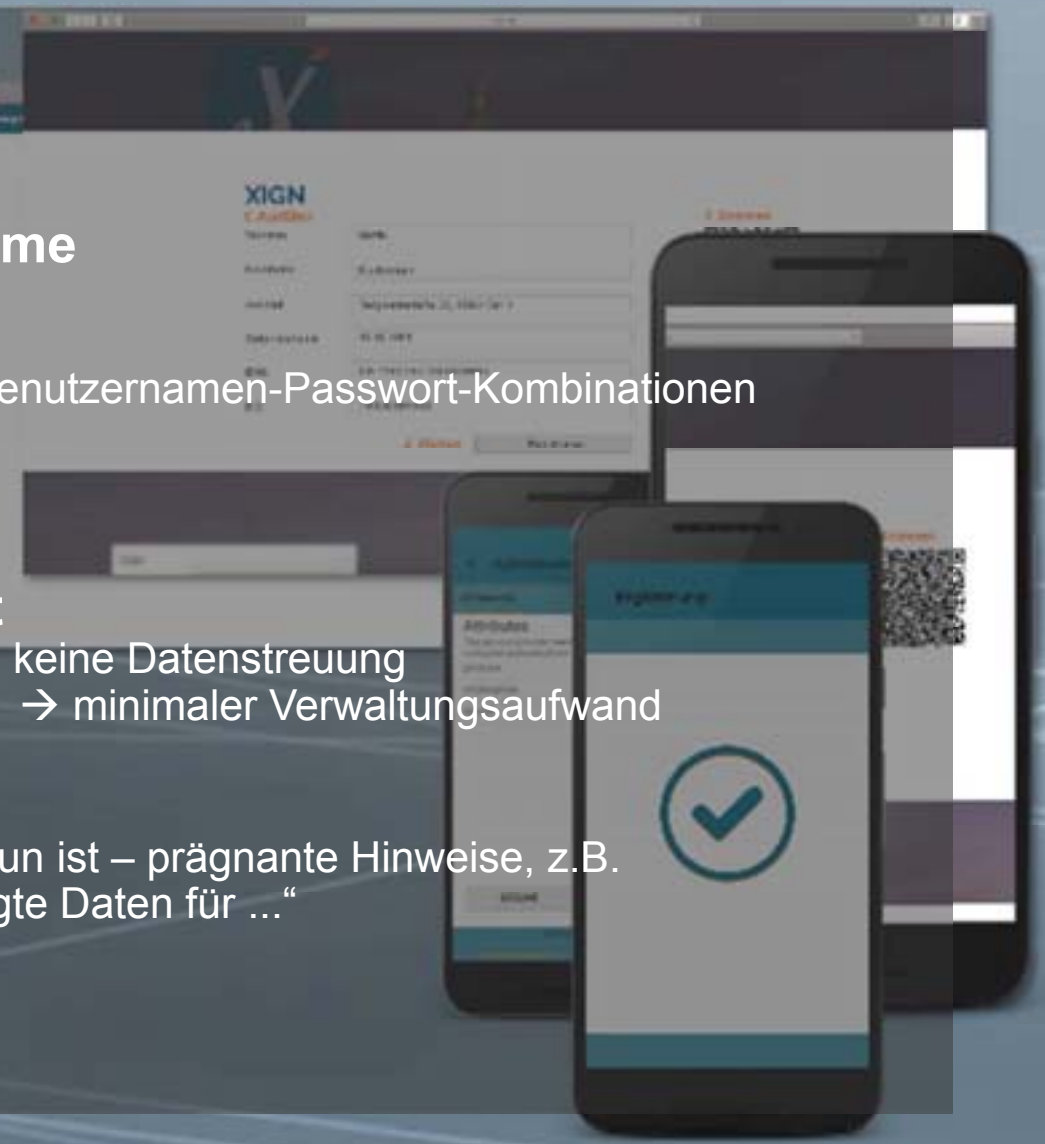
**→ Kosten- und aufwandsreduzierend**

# Produkt

## Vorteile – Nutzer

- **Keine zusätzlichen Schritte**
  - Nur noch Scannen und Bestätigen
- **Kein Passwort und Benutzername**
  - Weniger Interaktion
  - Kein Suchen oder „Probieren“ von Benutzernamen-Passwort-Kombinationen
- **Einfache Registrierung**
- **Datenhoheit** und **Verwaltbarkeit**
  - Eine Registrierung → ein Account → keine Datenstreuung → minimaler Verwaltungsaufwand
- **Gesteigertes Bewusstsein**
  - Weiß jederzeit was, wann, wieso zu tun ist – prägnante Hinweise, z.B. Ausführungsreihenfolge oder „benötigte Daten für ...“

→ **Bessere Nutzungserfahrung**



# Produkt

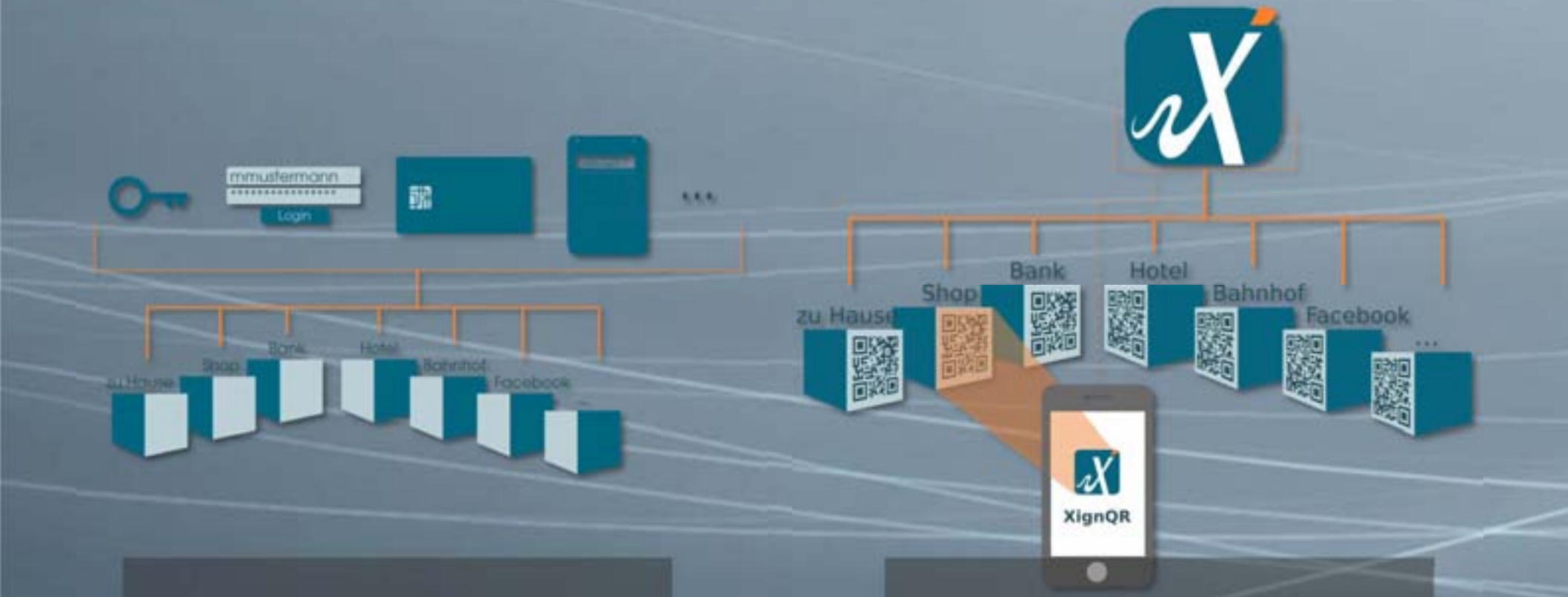
## Vorteile – Anbieter

- **Interoperabilität**
  - Ein System für zahlreiche Anwendungen, auch organsiationsübergreifend nutzbar
- **Einfache Integration**
  - Bedienen von Standards + Smartphone + QR Code
  - Client Library für nicht standardisierte Abläufe und Protokolle
- **Reduzierte Komplexität**
  - Verhindert Konfigurationsfehler und somit Sicherheitslücken
  - Ermöglicht das Einsparen von teuren Know-How
- **Einfache Wartbarkeit**
  - Schnelle Reaktion auf Änderungen und komfortables Risikomanagement
- **Gesteigerte Attraktivität**
  - Modern, Jung, Dynamisch


**→ Optimierte Businessprozesse bei gesteigerter Sicherheit und reduzierten Kosten**

# Produkt

## Vergleich – Authentifizierung & Signaturen




**Heutige Situation**

**XignQR Situation**

# Produkt

## Vergleich – Handel & Commerce

**Heutige**

**Situation**

**XignQR**

**Situation**

# Produkt

## Sicherheit

- Nicht anfällig für Brute-Force und Phishing, da kein Passwort
- Kontextbasierte Informationen erhöhen die Glaubwürdigkeit, Echtheit und Vertraulichkeit
- E2E-Verschlüsselung und mutual Authentication verhindern Man-In-The-Middle-Attacken und Datendiebstahl
- Schnelles und effizientes Risikomanagement (vgl. Verlust von EC-, Kredit-, SIM-Karte)

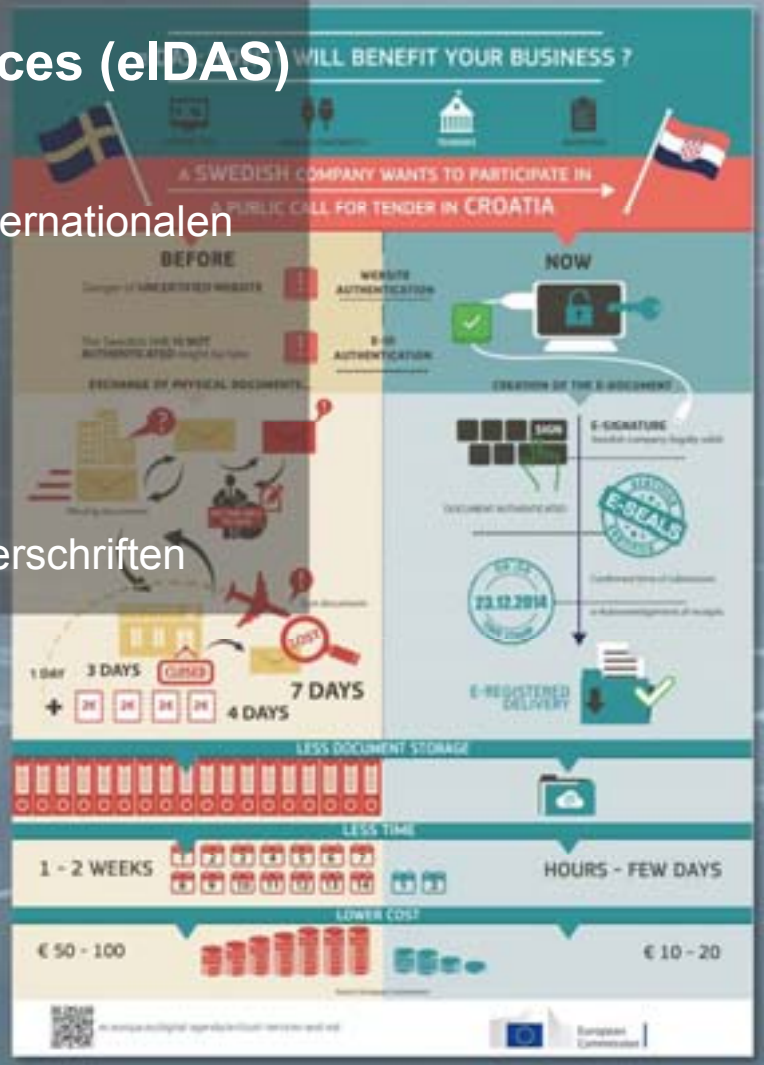
# Produkt
## Motivation

- **IT-Sicherheitsgesetz**
  - Bundesgesetz
  - Verpflichtet zur Meldung von IT-Sicherheitsvorfällen
  - Erhöht die Anforderungen an Unternehmen
  - Motiviert zu neuen Lösungen, Auslagerung und Nutzung von Kompetenzen
- **Schnelle Veränderungen im Markt**
  - Neue mobile Endgeräte vom PC zum Smartdevice und Wearables
  - Zusammenarbeit großer Unternehmen (z.B. FIDO Alliance) ermöglichen neue sichere und übergreifende Konzepte
- **NSA- & Snowden-Affäre**
  - Erschüttertet das Vertrauen in US-Technologie, durch das Aufzeigen von Sicherheitslücken, Hintertüren und Kompromittierung von Hardware


# Produkt

## Motivation – Signaturen und Tust Services

- **Electronic identification and trust services (eIDAS)**
  - Neue rechtlich anerkannte Signaturdienste
  - Erstmalige Chance* zum rechtsverbindlichen internationalen digitalen Handel
  - Gleichheit in allen Ländern der EU
- **Digitalisierung analoger Prozesse**
  - ermöglicht rechtsverbindliche elektronische Unterschriften

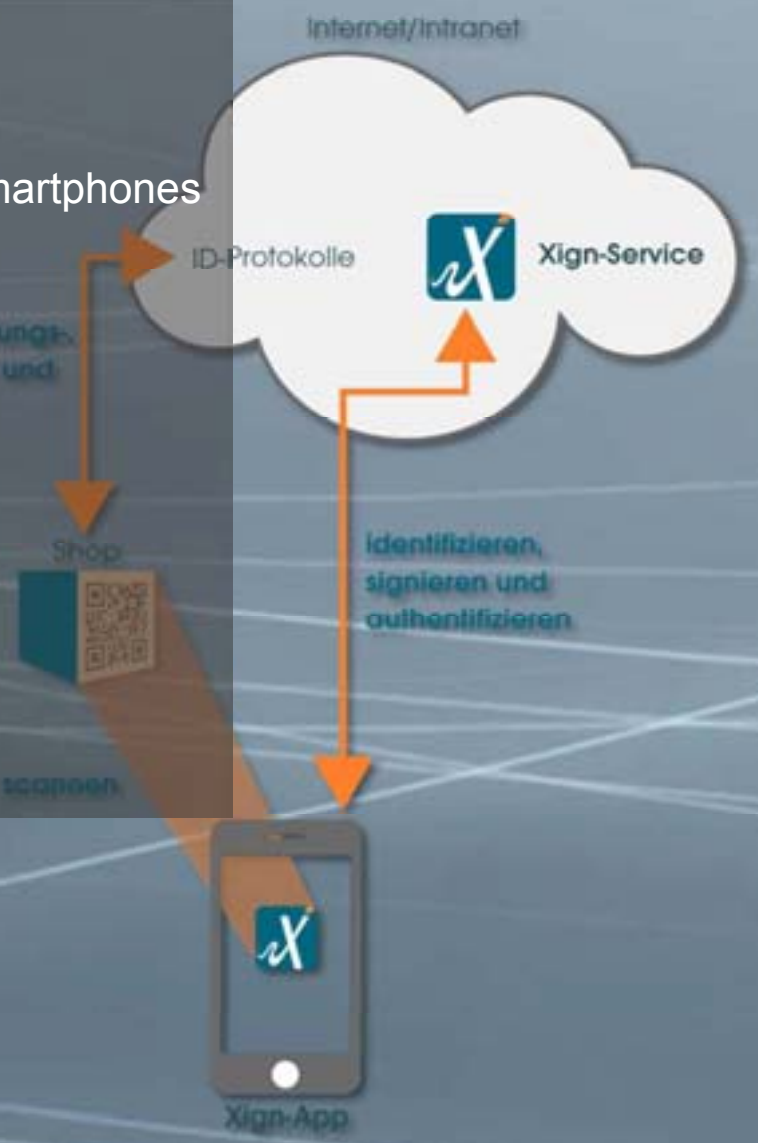


# Produkt

## Internet of the Things (IoT) & M2M

- **Infrastruktur as a Service – IaaS**
  - Nutzen der Schnittstellen des QR Code und des Smartphones
  - Modulares XignQR Design
  - Anbindung von Maschinen und andere Devices
  - Sichere, Vertrauenswürdige und nicht abstreitbare Kommunikation

**→ Nutzung für IoT und M2M-Kommunikation**



# Kontakt

Room for Questions

Wenn sie Fragen haben, zögern
sie nicht uns zu kontaktieren

Pascal Manaras – XignQR
Markus Hertlein – XignQR

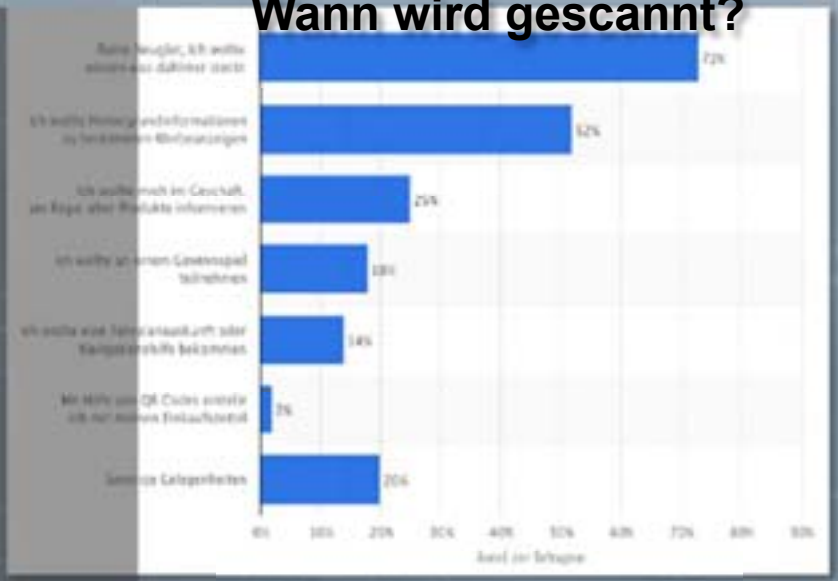
{manaras, hertlein}@xignqr.com

# Appendix

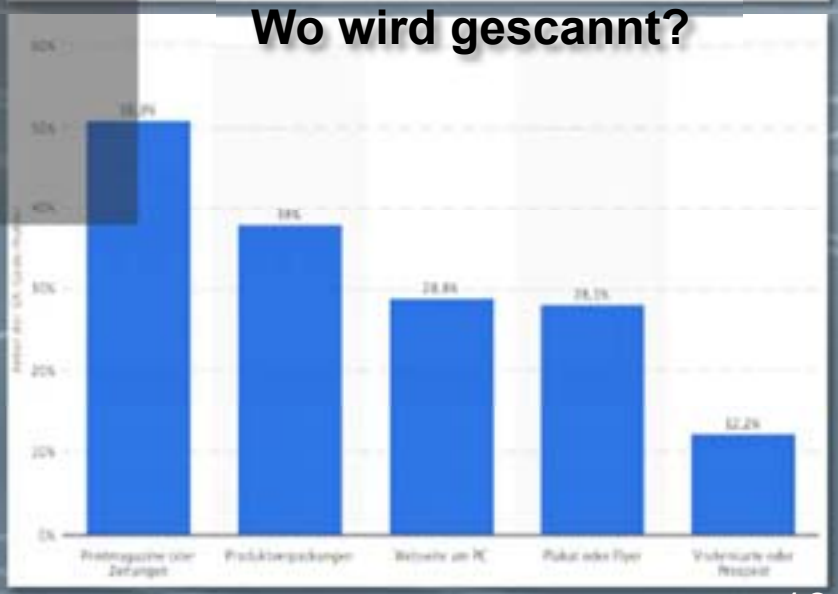
## Akzeptanz – QR Codes

- **2012 – 12% der Bevölkerung in Deutschland scannen QR Codes**
  - In den USA 40% der Bevölkerung
  - Deutschland bei QR Code Nutzung in der EU auf Platz 2 hinter Großbritannien
  - 20 % der Smartphone User in Deutschland
- **2015 – 29% der Bevölkerung scannen QR Codes**

**Wann wird gescannt?**

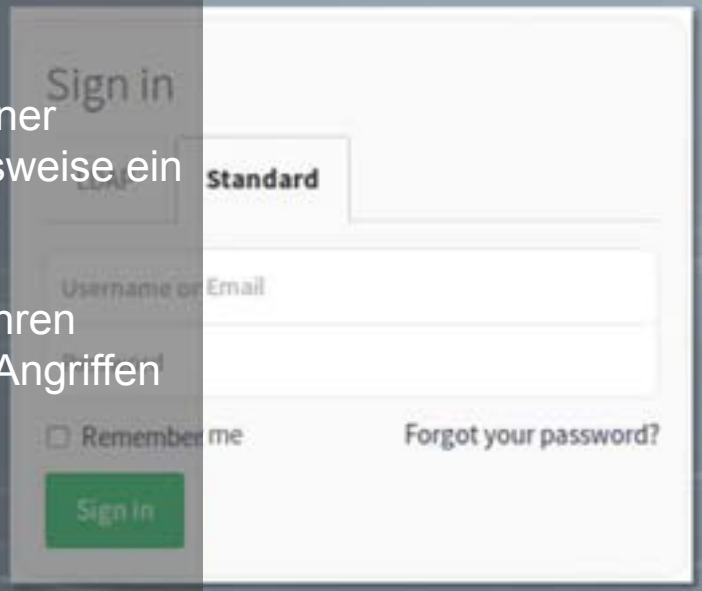


**Wo wird gescannt?**



# Appendix
## Grundlagen

- **Authentifizierung**
  - Authentifizierung ist der **Nachweis (Verifizierung)** einer behaupteten **Eigenschaft einer Entität**, die beispielsweise ein **Mensch** (...) sein kann
  - Häufig Authentifizierung über passwortbasierte Verfahren (Passwort / TAN / PIN): Anfällig für eine Vielzahl von Angriffen
- **Multifaktor Authentifizierung (MFA)**
  - Ziel: Verbesserung der Sicherheit von Authentifizierungsverfahren
  - Lösung: Authentifizierung über Kombination aus Wissen (z.B. Benutzername/Passwort) und Besitz (Smartphone) und/oder Sein (Biometrie)
  - Wesentliche Ansätze: One-Time-Passwords, Challenge Response




# Appendix
## Grundlagen

- **Security Token**
  - Sicherer Hardwarespeicher für kryptographisches Material
  - Verfügt über Algorithmen zum Signieren und Verschlüsseln
- **Lesegeräte / Cardreader**
  - Wird benötigt um mit Security Token zu kommunizieren
  - Gibt es in Ausführungen mit oder ohne Tastatur und Display
- **QR Code** (Quick Response Code – 2D Barcode)
  - Verfahren um Informationen in einer für Maschinen schnell zu verarbeitenden Form darzustellen
  - Kann jede Art von Information in codierter Form enthalten