



prisma cloud

# Durchsetzung von End-User-Sicherheit in Smart Services mittels Kryptographie

Vortrag auf der TA16-Konferenz in Wien, 20. Mai 2016

Thomas Länger  
thomas.laenger@unil.ch  
Université de Lausanne

Henrich C. Pöhls  
hp@sec.uni-passau.de  
Universität Passau

# Übersicht

- ▶ Unser Arbeits-Kontext - Das H2020 Projekt PRISMACLOUD
- ▶ Ziele des Projekts
- ▶ Informationssicherheit und Datenschutz in Cloud Diensten und Smart Services:
- ▶ Bedrohungen und Risiken aus Sicht der End-NutzerInnen
- ▶ Was sind Cloud Security Patterns?
- ▶ Präsentation von drei ausgewählten Cloud Security Patterns
- ▶ Rationale



prisma cloud

# Kontext: Das Projekt PRISMACLOUD

**PRISMACLOUD** ("Privacy and Security Maintaining Services in the Cloud") ist ein Horizon 2020-Forschungsprojekt der Europäischen Union (Dauer Feb. 2015 - Juli 2018) mit 16 Partnern und einem Fördervolumen von rund 8 Millionen Euro.

Das Projekt zielt darauf ab, heute weit verbreitete **gravierende Bedrohungen von Informationssicherheit und Privatsphäre** in aktuellen Cloud-Umgebungen durch kryptographische Verfahren abzumildern.

PRISMACLOUD will erreichen, dass kryptographische Verfahren im Sinne des **Privacy-by-Design-Ansatzes** gewissermaßen **von vornherein** in Cloud-Dienste eingebaut werden können.



prisma cloud

# Kontext: Das Projekt PRISMACLOUD (Forts.)

Die **kryptographischen Verfahren** werden in Form eines **Baukastens** zur Verfügung gestellt werden, wobei die einzelnen Elemente die kryptographischen Funktionen vollständig einkapseln.

Aus den einzelnen Elementen des Baukastens können dann Cloud-Dienste zusammengesetzt werden, wobei die Elemente an die **Funktionalität** und den **spezifischen Sicherheitsbedarf** individuell angepasst werden können.

Die heute weit verbreitete **Kompromittierung von Informationssicherheit und Privatsphäre** in Cloud-Diensten soll dadurch **wesentlich erschwert** werden.



prisma cloud

# Verhältnis von Cloud-Diensten und Smart Services

Dienstleistungen, basierend auf den gängigen **vernetzten, dynamischen Informationssystemen**:

- ▶ Cloud Dienste,
- ▶ Smart Services,
- ▶ Smart Products,
- ▶ Das „Internet der Dinge“

Es ergeben sich für die Endnutzerinnen in Bezug auf **Informationssicherheit und Datenschutz** ähnliche Bedrohungs-Szenarien – die **PRISMACLOUD Bausteine** haben auch im Smart-Services-Kontext Relevanz .



prisma cloud

# Informationssicherheit

## Allgemeine Betrachtungen:

- ▶ Vollständige oder absolute Informationssicherheit kann prinzipiell nicht hergestellt werden
- ▶ Informationssicherheit impliziert immer eine Abwägung zwischen dem Wert der zugrundeliegenden Daten und den Kosten eines Angriffs
- ▶ Aussagen zu Informationssicherheit können nur in Relation zu bestimmten Sicherheitszielen getroffen werden
- ▶ Sicherheitsziele in einem Kontext sind relativer Natur, bezüglich unterschiedlicher Akteure



prisma cloud

# Bedrohungen und Risiken aus Sicht der EndnutzerInnen

## Taxonomie von Risiken:

1. Privatsphäre-Risiken
2. Kontrolle und Organisation betreffende Risiken
3. Technische Risiken

### 1. Privatsphäre-Risiken (Auswahl)

- ▶ Verlust der Vertraulichkeit privater Information
- ▶ Örtliche und zeitliche Nicht-Lokalität von Daten
- ▶ Verletzung von Datenschutzgesetzen
- ▶ Persistenz von Information in Informationssystemen
- ▶ Unvollständige Löschung von Daten
- ▶ Implizite Generierung von Meta-Daten



prisma cloud

# Bedrohungen und Risiken (Forts.)

## 2. Kontrolle und Organisation betreffende Risiken (Auswahl)

- ▶ Persönliche Daten werden aus dem Wirkungsbereich einer Datenschutz-Gesetzgebung verschoben
- ▶ Kontrollverlust bezüglich der Einhaltung von Sicherheitspolitiken bzw. Geschäftsbedingungen
- ▶ Verletzung der Sorgfaltspflicht durch den Dienstleister
- ▶ Kontrollverlust über tatsächliche Verarbeitung
- ▶ Fehlende Interventionsmöglichkeit der EndnutzerInnen
- ▶ „Lock-in“ in Dienste
- ▶ Übernahme von Profilen durch Unbefugte
- ▶ Verlust der Verfügbarkeit von Daten („Denial of Service“)
- ▶ Insolvenz des Dienstleisters





# Bedrohungen und Risiken (Forts.)

## 3. Technische Risiken (Auswahl)

- ▶ Fehler im Programmcode (Spezifikation, Implementierung)
- ▶ Fehlerhafte Konfiguration
- ▶ Kompromittierung von Schnittstellen
- ▶ Unzureichende Mandantentrennung
- ▶ Verlust der Intaktheit von Information
- ▶ Datenverlust
- ▶ Unzureichende kryptographische Sicherheit



# Cloud Security Patterns

Verwendung von **Cloud Security Patterns** für die Analyse von **typischen Situationen, in denen Informationssicherheits- und Datenschutz-Probleme auftreten** – und welche kryptographischen Funktionalitäten angewendet werden können, um diese Probleme abzumildern

**Cloud Security Patterns** sind ein Anwendung von **Design Patterns** und beschreiben wiederverwendbare, erprobte Lösungen (mittels der vorgeschlagenen „Bausteine“) für wiederkehrende Probleme

**Charakterisierung nach Kategorien:** Name des Patterns, kurze Beschreibung, Kontext, Intention, Problem, Lösung, Konsequenzen



prisma cloud

# Cloud Security Patterns (Forts.)

## Cloud Security Patterns

- ▶ sind deskriptiv statt normativ
- ▶ kommunizieren oftmals widersprüchliche Sicherheitsanforderungen verschiedener Beteiligter
- ▶ sensibilisieren für das Vorhandensein kontradiktorischer Aspekte
- ▶ ermöglichen einen Diskussionsprozess
- ▶ beschreiben generative Lösungen für Design-Konflikte
- ▶ unterstützen einen Security-by-Design-Ansatz



prisma cloud

# Pattern 1: „Standardmäßige sichere Datenspeicherung“

## Problem:

- ▶ Daten werden hauptsächlich unverschlüsselt gespeichert
- ▶ Dienstleister haben vollen Zugriff
- ▶ Sicherheit ist oftmals nur durch Geschäftsbedingungen geregelt
- ▶ Verfügbarkeit der Daten ist keineswegs gesichert
- ▶ Effektive Löschung von Daten ist nicht möglich
- ▶ „Lock-In“ erschwert Dienstleister-Wechsel
- ▶ Ende-zu-Ende-Verschlüsselung beeinträchtigt Teilen von Daten

## Baustein: „Sicherer Objekte-Speicher“

- ▶ Anwendung eines „Secret Sharing Protokolls“
- ▶ Daten werden in mehrere Fragmente zerlegt
- ▶ Fragmente werden auf mehrere Dienstleister aufgeteilt
- ▶ Information kann nur mit einer definierten Anzahl von Teilen rekonstruiert werden („threshold scheme“)



prisma cloud

# Pattern 1: „Standardmäßige sichere Datenspeicherung“ (Forts.)

## Eigenschaften:

- ▶ Einzelner Dienstleister hat keinen Zugriff auf die Klardaten
- ▶ Baustein bietet (nachweisbare) kryptographische Sicherheit ohne Schlüssel
- ▶ Verfügbarkeit der Daten, auch bei Ausfall von Dienstleistern
- ▶ End-User kann beliebige Teile „devalidieren“ und neue Teile generieren (verhindert „Lock-In“)



# Pattern 2: ‘Nicht-identifizierbare und nicht-verfolgbare Nutzung eines Dienstes‘

## Problem:

- ▶ Herkömmliche Authentifizierung für Dienste mittels Identitäts-Zertifikat impliziert die Offenlegung der Identität
- ▶ Herkömmliche Authentifizierung enthüllt sämtlich im Zertifikat vorgelegte Daten
- ▶ Daten können gesammelt werden und ohne möglich Kontrolle des Daten-Subjekts weiterverarbeitet werden

## Baustein: „Authentifizierung mit selektiver Offenlegung“

- ▶ Anwendung von „attribute based credentials“ (Attribut-basierten Zugangsdaten)



prisma cloud

## Pattern 2: „Nicht-identifizierbare und nicht-verfolgbare Nutzung eines Dienstes“ (Forts.)

- ▶ Die BenutzerIn übermittelt einem Aussteller diverse Attribute und erhält von diesem ein „attribute based credential“
- ▶ Die BenutzerIn kann mit Hilfe dieses credentials einem Überprüfer („verifier“) beweisen, dass sie ein bestimmtes Attribut besitzt, ohne ihre Identität aufzudecken.
- ▶ Die BenutzerIn kann dem Überprüfer bestimmte Eigenschaften eines Attributs beweisen, ohne das Attribut offenzulegen

### Eigenschaften:

- ▶ Ermöglicht die anonyme oder pseudonyme Autorisierung für einen Dienst
- ▶ Ein „multi-show credential system“ ermöglicht mehrere unverknüpfbare Interaktionen mit dem Überprüfer
- ▶ Effektive Umsetzung des Prinzips der Datensparsamkeit bzw. Datenvermeidung



prisma cloud

# Pattern 3: „Kontrollierte Modifikation von signierten Daten“

## **Problem:**

- ▶ Die Veränderung von signierten Daten zerstört üblicherweise die Authentizitäts-Eigenschaft der Daten
- ▶ Einzelne Daten (die nicht übermittelt werden sollen) können nicht unterdrückt werden

## **Baustein: „Authentifizierung mit selektiver Offenlegung“**

- ▶ Verwendung von editierbaren Signaturen („malleable sign.“)
- ▶ Es können Untermengen der signierten Daten erzeugt werden, ohne die Gültigkeit der Signatur zu zerstören
- ▶ Es können (erlaubte) Modifikationen an den Daten vorgenommen werden, ohne die Gültigkeit der Signatur zu zerstören
- ▶ Die „erlaubte“ Bildung von Untermengen und Modifikationen wird durch eine Sicherheitspolitik beschränkt



prisma cloud



# Pattern 3: „Kontrollierte Modifikation von signierten Daten“ (Forts.)

## Eigenschaften:

- ▶ Die Weitergabe wird nach dem Prinzip der Datensparsamkeit auf die notwendigen Daten beschränkt
- ▶ Modifikationen können für jede/n erlaubt werden, oder nur für Parteien, die im Besitz eines bestimmten Signaturschlüssels sind
- ▶ Erlaubte Modifikationen können auf bestimmte arithmetische Funktionen beschränkt werden
- ▶ Die Ursprungseigenschaft von Änderungen kann kryptographisch verifiziert werden (Zuordenbarkeit)
- ▶ Editierbare Signaturen entsprechen (unter bestimmten kryptographischen Bedingungen) qualifizierten elektronischen Signaturen nach deutschem SigG und der eIDAS-Verordnung



# Weitere Bausteine

Im Rahmen des Projekts werden 6 weitere Pattern beschrieben, welche auf den Funktionalitäten von 3 weiteren Bausteinen basieren:<sup>1</sup>

- ▶ Baustein: **Verifizierbare Datenverarbeitung**
  - ▶ Ermöglicht die Verifizierung von bestimmten erlaubten Operationen auf signierten Daten (Korrektheit)
  - ▶ Ermöglicht die Delegation von Berechnungen auf signierten Daten
- ▶ Baustein: **Topologie-Zertifizierung**
  - ▶ Graph-Signaturen ermöglichen, basierend auf Graphen, die Signatur von Topologien virtueller Infrastrukturen
  - ▶ Eigenschaften von Graphen (z.B. Isolation von virtuellen Infrastrukturen verschiedener Kunden) können über diese Signaturen nachgewiesen werden

---

<sup>1</sup>Siehe Publikationen und Deliverables auf [prismacloud.eu](http://prismacloud.eu)



# Weitere Bausteine (Forts.)

## ▶ **Daten-Privatsphäre-Tool**

- ▶ Ermöglicht die Anonymisierung großer Datenmengen (z.B. für klinische Studien)
- ▶ Anwendung des kryptographischen Primitives „k-Anonymität“
- ▶ Es gibt dann immer mindestens  $(k-1)$  Datensätze, die von denen ein bestimmter Datensatz nicht unterschieden werden kann



prisma cloud

# Rationale

## Zusammenfassende Punkte:

- ▶ Kryptographische Funktionalitäten können die Bedrohungen von Informationssicherheit und Privatsphäre effektiv reduzieren
- ▶ Kryptographische Funktionen können nach den Prinzipien des Privacy-by-designs von vornherein in vernetzten Diensten vorgesehen werden
- ▶ Das Prinzip der Datensparsamkeit kann ebenfalls unterstützt werden

## Motivationen für die Verwendung der vorgeschlagenen Bausteine:

- ▶ Standardisierung
- ▶ als Basis für Regulation
- ▶ Kompetitiver Vorteil von Anbietern von abgesicherten und datensparenden Diensten



prisma cloud

# Wir Danken für Ihre Aufmerksamkeit!

Thomas Länger  
thomas.laenger@unil.ch  
Universität de Lausanne

Henrich C. Pöhls  
hp@sec.uni-passau.de  
Universität Passau

H2020-Projekt **PRISMACLOUD**  
[www.prismacloud.eu](http://www.prismacloud.eu)



prisma cloud