

# OSCI (!)

- Was ist OSCI?
  - Warum wurde OSCI entwickelt?
  - Wie funktioniert OSCI?
- 

## Was ist OSCI?

OSCI ist eine plattformunabhängige Sammlung von Netzwerkprotokollen der deutschen öffentlichen Verwaltung für die sichere, vertrauliche und rechtsverbindliche Übertragung elektronischer Daten im E-Government. Der Standard wurde von der Koordinierungsstelle für IT-Standards (KoSIT) entwickelt, ist lizenzfrei und darf kostenlos verwendet werden. Das zugrundeliegende Transportprotokoll besteht aus Webdiensten auf der Basis internationaler Standards (z.B. SOAP, WS-Stack) und enthält zudem optionale Funktionen die im deutschen E-Government insbesondere Nachweise im Transport der Daten benötigt werden. OSCI erlaubt die digitale Signatur und die Verschlüsselung des jeweiligen Inhalts.

[blocked URL](#)

[\(zurück\)](#)

---

## Warum wurde OSCI entwickelt?

OSCI wurde entwickelt um die klassischen Schutzziele Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit bei der Übermittlung von Nachrichten in unsicheren Netzen (z.B. das Internet) zu gewährleisten. Weiterhin war die Interoperabilität mit verschiedenen Systemen und Technologien ein treibender Faktor.

Bei der Nutzung von OSCI stellte sich schnell heraus, dass die Implementation von kryptografischen Methoden insbesondere für mittlere und kleinere IT-Hersteller von Antrags- und Fachverfahren eine unüberbrückbare Hürde darstellt. Deswegen wurde OSCI zu einem späteren Zeitpunkt durch den Standard [XTA](#) ergänzt, welcher die Verschlüsselung der Nachrichten aus dem Fachverfahren übernimmt.

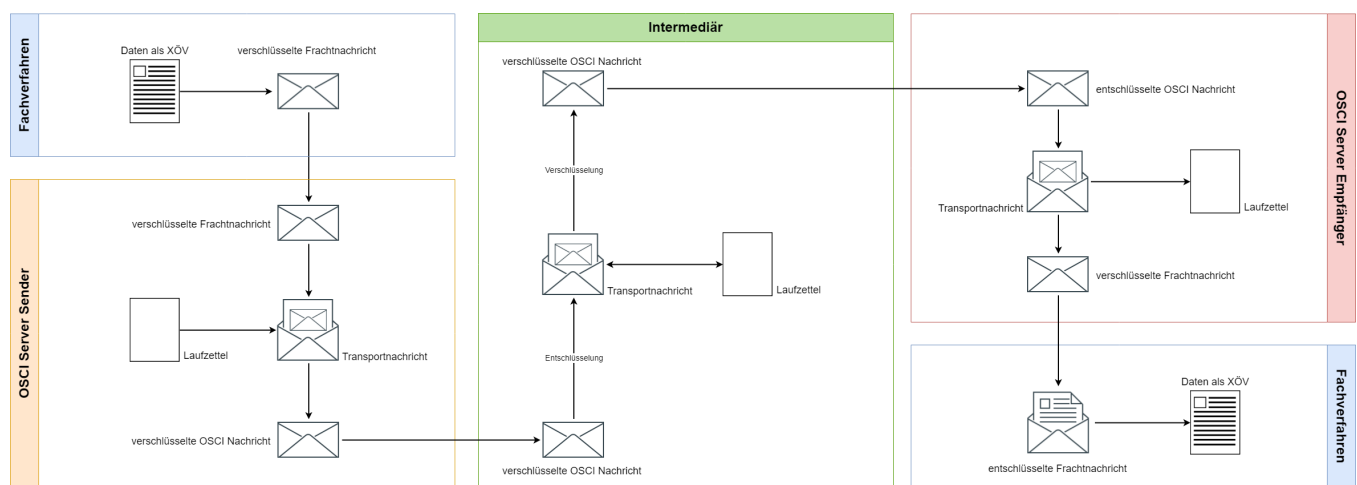
[\(zurück\)](#)

---

## Wie funktioniert OSCI?

Die hier abgebildete Vorgehensweise erläutert OSCI ohne die Erweiterung [XTA](#) (!).

OSCI Nachrichten haben einen zweistufigen "Sicherheitscontainer". Dadurch ist es möglich Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptografisch unterschiedlich zu behandeln. Die Inhaltsdaten werden vom Autor einer OSCI-Nachricht so verschlüsselt, dass nur der berechtigte Leser sie dechiffrieren kann. Die Nutzungsdaten werden vom Intermediär für die Zwecke der Nachrichtenvermittlung und die Erbringung von Mehrwertdiensten. Der Intermediär kann aber nicht auf die Inhaltsdaten zugreifen. Oft wird hier vom Prinzip des "Doppelten Umschlages" gesprochen.



[\(zurück\)](#)