Authentifikation von Webseiten

Sichere Webseiten, bei denen der Betreiber authentifiziert werden kann, erkennt man daran, dass sie das Protokoll *https* verwenden und im *Internet Explorer* neben der Adresszeile ein kleines Schloss angezeigt wird. In diesem Fall wird das Zertifikat des Betreibers beim Aufruf der Webseite automatisch mitgesendet und überprüft.

Aufgabe 1: Öffnen Sie im *Microsoft Internet Explorer* die Webseite <u>https://www.amazon.de</u> und klicken Sie auf das kleine Schloss rechts neben der URL: Klicken Sie in dem sich öffnenden Fenster auf *Zertifikate anzeigen*. Verschaffen Sie sich anhand der Unterfenster *Allgemein* und *Details* welche Informationen in einem Zertifikat enthalten sind. Sie können die Aufgabe natürlich auch mit einem anderen Browser bearbeiten. Im *Mozilla Firefox* befindet sich z. B. links neben der URL ein kleines Schlosssymbol. Über *Weitere Informationen* \rightarrow *Zertifikat anzeigen* gelangt man zu denselben Informationen.

In der Regel müssen Sie nicht selbst überprüfen, ob der Betreiber einer Webseite ein gültiges Zertifikat besitzt. Diese Aufgabe übernimmt der Browser. Dazu verfügt der Browser bereits bei der Auslieferung über die öffentlichen Schlüssel aller vertrauenswürdigen Zertifizierungsstellen (s. Abbildung. 3). Sie können sich diese Liste anschauen, wenn Sie in den Internetoptionen (IE) bzw. den Einstellungen (Firefox) den Button Zertifikate bzw. Zertifikate anzeigen anklicken.

| In | iternetoptionen 🤶 🔯 | E | instellungen | | | / | | | | × |
|----|--|---------|--------------|---------------------------|---------------------|------------------|---------------------------|------------------------|-----------|---------------|
| | Verbindungen Programme Erweitert Allgemein Sicherheit Datenschutz Inhalte | | Allgemein | Tab | Inhalt | Anwendunger | Datenschut | tz Sicherheit | Sync Sync | Erweitert |
| | Family Safety Steuert die Internetinhalte, die angezeigt werden dürfen. Zertrifikate | \succ | Wenn eine | Website na atisch eins | ch dem pe wählen | ersönlichen Sich | erheitszertifikat agen | verlangt: | | |
| | Für verschlüsselte Verbindungen und zur Identisserung werden Zertifikate verwendet. SSL-Status löschen Zertifikate Herausgeber AutoVervollständigen | | Zertifikate | anzeigen | Ze <u>r</u> tifik | atsperrliste | <u>V</u> alidierung | <u>K</u> ryptographie- | Module | |
| | AutoVervollständigen speichert vorherige Eingaben auf Webseiten und schlägt Übereinstimmungen vor. Feeds und Web Slices | | | | | | | | | |
| | Einstellungen aktualisierte Inhalte von Websites, die in Internet Explorer und anderen Programmen gelesen werden können. | | | | | | | | | |
| | | | | | | | ОК | Abbrech | en | <u>H</u> ilfe |
| | | | Abbildur | ig 2: Mo | ozilla Fi | irefox | | | | |
| | OK Abbrechen Übernehmen | | | | | | | | | |

Abbildung 1: Microsoft Internet Explorer

| wischenzertifizierungsstelle | n Vertrauenswürdige Sta | mmzertifizierun | gsstellen Vertrauen: |
|--|-----------------------------|-----------------|----------------------|
| Ausgestellt für | Ausgestellt von | Ablaufda | Anzeigename |
| 🛱 AddTrust External | AddTrust External CA | 30.05.2020 | USERTrust |
| 🔄 Baltimore CyberTru | Baltimore CyberTrust | 13.05.2025 | Baltimore Cyber |
| 🔄 Certum CA | Certum CA | 11.06.2027 | Certum |
| 🔄 Class 3 Public Prima | Class 3 Public Primary | 02.08.2028 | VeriSign Class 3 |
| 🔄 Class 3 Public Prima | Class 3 Public Primary | 08.01.2004 | VeriSign |
| 🔄 Copyright (c) 1997 | Copyright (c) 1997 Mi | 31.12.1999 | Microsoft Timest |
| 🔄 Deutsche Telekom | Deutsche Telekom Ro | 10.07.2019 | Deutsche Teleko |
| DigiCert Assured ID | DigiCert Assured ID R | 10.11.2031 | DigiCert |
| DigiCert High Assur | DigiCert High Assuran | 10.11.2031 | DigiCert |
| nportieren Exportieren | n Entfernen | | Erweiter |
| eabsichtigte Zwecke des Ze | ertifikats | | |
| erverauthentifizierung. Clie | ntauthentifizierung. Sicher | e E-Mail Code | signatur |
| eitstempel, Verschlüsselnde P-Sicherheitsbenutzer | es Dateisystem, IP-Sicherhe | eitstunnelabsch | nluss, Anzeiger |

Abbildung 3: Im Microsoft Internet Explorer gespeicherte vertrauenswürdige Zertifizierungsstellen.

Solange ein Zertifikat von einer dieser vertrauenswürdigen Instanzen ausgestellt wurde, stuft der Browser die Webseite als sicher ein und zeigt sie wie gewohnt an. Nur wenn der Browser feststellt, dass der Aussteller eines Zertifikats unbekannt ist, erscheint eine entsprechende Meldung im Browser.

Aufgabe 2:

- a) Geben Sie die URL https://webmail.gmx.de im Browser ein und versuchen Sie die Seite zu öffnen. Es müsste eine Meldung wie in Abbildung 4 oder 5 erscheinen.
- b) Diskutieren Sie für den Fall, dass beim Aufruf einer Webseite die Meldung aus Abbildung 4/5 erscheint, mögliche Vorgehensweisen und ihre Auswirkungen.



Abbildung 4: Fehlermeldung bei Zertifikaten unbekannter Zertifizierungsstellen im IE.

| https://w | ebmail.gmx.de |
|-----------|---|
| | Dieser Verbindung wird nicht vertraut Sie haben Firefox angewiesen, eine gesicherte Verbindung zu webmail.gmx.de aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden. Was sollte ich tun? Talls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass immand die Website fälscht. Sie sollten in dem Fall nicht fortfahren. Diese Seite verlassen Ich kenne das Risiko |

Abbildung 5: Fehlermeldung bei Zertifikaten unbekannter Zertifizierungsstellen im Firefox.