Übungsblatt 8

8.1

a)

pure: ein Name ist nur ein Bit-Muster und enthält keinerlei wetere Information

bsp: UUIDs als Namen von DCOM-Objekten oder Klassen

impure: ein Name implzert zusätzliche Informationen über das bezeichnete Objekt

bsp: DNS-Namen (mail.informatik.fh-wiesbaden.de)

b) ein Name wird als unique bezeichnet, wenn er eindeutig (also höchstens) ein Objekt identifiziert

bsp1: Daniel Mattes -> nicht unique (mit Geburtstag und Geburtsort schon)

bsp2: UUID (Globally Unique Identifier)

8.2

a)Ebenen:

-Global Layer (High-Level Knoten -> Enstiegspunkte)

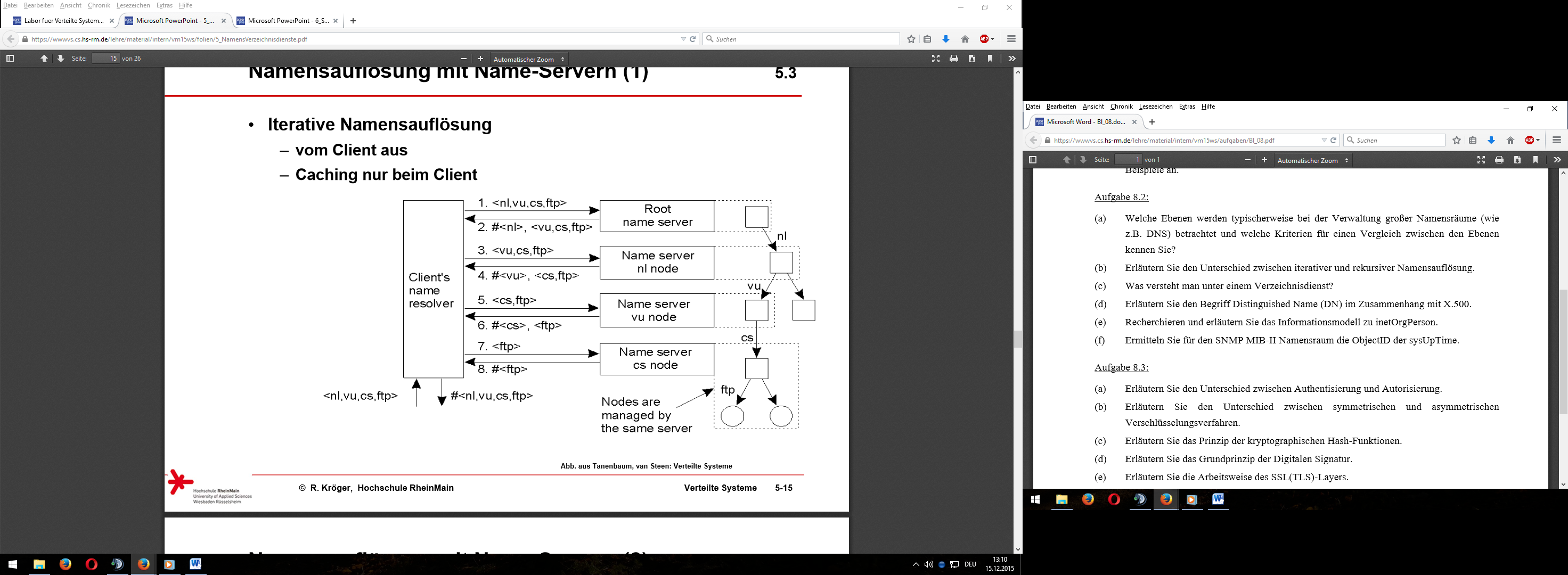
-Administrative Layer (Namensräume innerhalb ener Organsation)

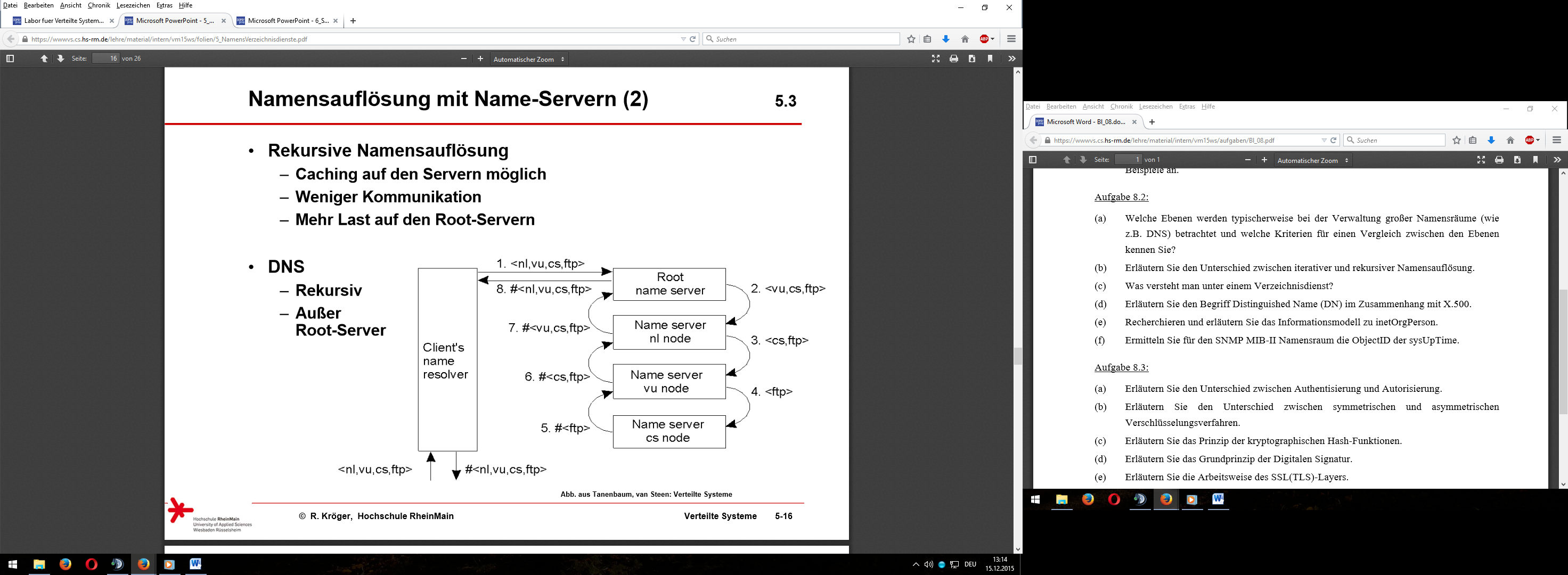
-Managerial Layer (Namensräume mit Namen, die sich häufig ändern)

Kriterien für den Vergleich:

-

b)





c) ein Verzeichnisdienst ist wie ein Telefonbuch zu verstehen.

Einträte werden hier in erster Linie über Eigenschaften statt über Namen gesucht.

d) Der Ausgangspunkt ist ein DIT (Directory Information Tree).

Dort hat jeder Knoten in seiner Ebene einen eindeutigen Namen(Relative Distinguished Name (RDN)).

Die Zusammensetzung der RDNs vom Knoten bis zur Wurzel heißt dann Distinguished Name (DN).

Im Zusammenhang mit X.500: ……….

e)

f) 1.3.6.1.2.1.1.3

8.3

a)

Authentisierung: wer möchte etwas?

Autorisierung: darf er das?

b)

symmetrisch: ein einziger key zum Ver- und Entschlüsseln

asymmetrisch: ein privater key zum Lesen, aber ein öffentlicher Key zum Verschlüsseln

c),d) eine kryptographische Hash-Funktion dient als digitale Signatur.

Die Ausgangsnachricht wird über eine Hash-Funktion verschlüsselt und so in eine Bitkette bestimmter Länge umgewandelt. Von dem Hash-Wert auf die Ausgansnachricht zu kommen ist extrem rechenaufwändig.

Der Empfänger der Nachricht kann diese dann ebenfalls mit der Selben Hash-Funktion verschlüsseln und überprüfen, ob diese Bitkette mit der empfangenen übereinstimmt.

f)Für gewöhnlich schickt der Client zum Verbindungsaufbau einen Request an den Server. Dieser schickt als Antwort das Zertifikat und die Präferenzen für das Verschlüsselungsverfahren.

Daraufhin kann der Client einen Master Key erzeugen und mithilfe des im Zertifikat enthaltenen public Keys verschlüsselt an den Server senden.

Der Server entschlüsselt jetzt den Master Key und authentifiziert sich gegenüber dem Client, in dem er eine mit dem Master Key verschlüsselte Antwort-Nachricht sendet.

Ab hier werden dann nur noch Keys benutzt, die aus dem Master Key abgeleitet sind.