<VORNAME> <NACHNAME>

Investigating Adaptive Rate Control in NDN-RTC

MASTERARBEIT

zur Erlangung des akademischen Grades
Diplom-Ingenieur

STUDIUM
Angewandte Informatik

Alpen-Adria-Universität Klagenfurt
Fakultät für Technische Wissenschaften

BEGUTACHTER
Assoc.Prof. Dr. Peter Schartner

Institut für Angewandte Informatik
Forschungsgruppe Systemsicherheit

Version <0.01 – 0.99>

Klagenfurt, <DATUM DER ABGABE>

In case of comments or problems, please contact the System Security Research Group (info@syssec.at) or the author (<**EMAIL**>).

Zitat, falls gewünscht
von wem?

Affidavit

I hereby declare in lieu of an oath that

- the submitted academic paper is entirely my own work and that no auxiliary materials have been used other than those indicated;
- I have fully disclosed all assistance received from third parties during the process of writing the paper, including any significant advice from supervisors;
- any contents taken from the works of third parties or my own works that have been included either literally or in spirit have been appropriately marked and the respective source of the information has been clearly identified with precise bibliographical references (e.g. in footnotes);
- to date, I have not submitted this paper to an examining authority either in Austria or abroad and that
- the digital version of the paper submitted for the purpose of plagiarism assessment is fully consistent with the printed version.

I am aware that a declaration contrary to the facts will have legal consequences.

<SIGNATURE> Klagenfurt, **<DATE>**)

Acknowledgements

Unser Dank gilt Raphael Wigoutschnigg, da diese Vorlage für wissenschaftliche Arbeiten der Gruppe Systemsicherheit (syssec) auf den LaTeX-Files seiner Diplomarbeit aufbaut.

Abstract

Diese Arbeit beschäftigt sich mit der vorgeschlagenen Formatvorlage für wissenschaftliche Arbeiten der Forschungsgruppe Systemsicherheit. Es steht Ihnen selbstverständlich frei, die Vorlage an Ihre Bedürfnisse (und Ihren Geschmack) anzupassen. Zudem enthält dieser Text einige spezielle Tipps und Richtlinien für DiplomandInnen. Falls Sie Fehler entdecken, Wünsche oder Anregungen bzgl. der Formatvorlage haben, so senden Sie diese bitte per eMail an peter@syssec.at).

Wichtige Hinweise

- Diese Vorlage kann ohne Änderungen mittels PDFLaTeX von MikTeX compiliert werden. Daher müssen auch die Abbildungen als PDF vorliegen.
- Muss zur Compilierung aber LaTeX genutzt werden, da psfrag (oder Ähnliches verwendet wird),dann darf das Package hyperref nicht verwendet werden → Package hyperref (inkludiert am Beginn dieser Datei) auskommentieren und \newcommand{\href}[2]{#2} definieren. Abbildungen müssen dann als eps vorliegen.
- Damit das Literaturverzeichnis erzeugt wird, muss "bibtex thesis" aufgerufen werden.
- Damit das Abkürzungsverzeichnis erzeugt wird, muss "nomenclature.bat" aufgerufen werden.
- Einige Dokumente die den Umgang mit LaTeX und diversen Packages beschreiben, finden Sie im Verzeichnis "README".
- Textstellen (wie Datumsangeben oder Namen) die anzupassen sind, wurden teilweise mit Platzhaltern der Form <**BESCHREIBUNG**> versehen! Nicht markierte Stellen der Titelseite, die gegebenenfalls anzupassen sind, umfassen
  - Bezeichnung des Studiums und
  - Name der betreuenden Assistentin bzw. des betreuenden Assistenten.
- Vor dem Ausdruck für die gebundene Masterarbeit ist die boolesche Variable "FINAL" (siehe Zeile 49 in dieser Datei) auf "true" zu setzen! Nicht ersetzte Platzhalter – das sind Kommandos der Form \ph{...} – werden dann beim Aufruf von PDFTex zu einer Fehlermeldung führen.
- Die aktuelle Version dieses Dokuments finden Sie auf http://www.syssec.at/downloads/.

Table of Contents

Grundlagen

Dieses Kapitel soll einen sanften Einstieg in den Bereich der Smartcards bieten. Aus diesem Grund wird zu Beginn dieser Arbeit auf die verschiedenen Hardwaretypen eingegangen. Da eine Chipkarte ohne Lesegerät wie der Fisch ohne Wasser ist, wird auch diese Hardwarekomponente behandelt. Um die Allgegenwart von Chipkarten zu veranschaulichen, wird schlussendlich ein Einblick in die Einsatzmöglichkeiten dieser Mini-Computer gegeben.

Informationen zu diesem Kapitel sind, wenn nicht anders angegeben, den beiden Standardwerken aus dem Bereich Chipkarten "'Handbuch der Chipkarten"' [RaEf02] und "'Chipkartenanwendungen"' [Rank06] entnommen.

Typen von Chipkarten

Aufgrund der vielen Einsatzmöglichkeiten von Chipkarten, die mehr oder weniger Sicherheit bzw. mehr oder weniger Mobilität verlangen, kann man Chipkarten nach zwei Gesichtspunkten – dem Chiptyp und der Datenübertragung– unterscheiden. Anhand des Chiptyps werden die Karten in Speicher- und Prozessorchipkarten unterteilt, wogegen sie durch die Datenübertragung in kontaktbehaftete, kontaktlose und Dual-Interface Karten aufgegliedert werden.

Prozessorchipkarten haben im Unterschied zu Speicherchipkarten sehr viel stärkere Sicherheitsmaßnahmen implementiert und dienen als kleine Datentresore. Kontaktbehaftete Karten können nur von einem geeigneten Lesegerät mit Steckvorrichtung gelesen werden. Dagegen ist bei kontaktlosen Karten die Kommunikation nur über die Luftschnittstelle möglich. Dual-Interface Karten sind eine Kombination aus diesen zwei Typen und beherrschen beide Übertragungstechniken. Diese Diplomarbeit beschäftigt sich zum größten Teil mit Prozessorchipkarten und geht auf Speicherchipkarten nur insoweit ein, um dem Leser den Unterschied zwischen diesen zu erklären.

Speicherchipkarten

Speicherchipkarten haben eine sehr einfache Logik, die es lediglich erlaubt, Daten in den Speicherbereich auf der Karte zu schreiben und diese wieder zu lesen. Es sind sehr schwache Sicherheitsmaßnahmen (z.B. keine Erhöhung des Restbetrages bei Wertkarten für Telefonzellen) zum Schutz der Daten vorhanden, wodurch sie für Hochsicherheits-Anwendungen ungeeignet sind. Durch die geringen Sicherheitsanforderungen benötigen diese Karten auch keinen teuren (Co-)Prozessor. Es sind lediglich EEPROM, ROM und eine Speicherverwaltung mit eventuell integrierter Sicherheitslogik notwendig. Speicherchipkarten sind auch nicht derart stark gegen physikalische Angriffe gewappnet, wie das die hochwertigen Prozessorkarten sind. Durch dieses

einfache Design ist ihr Preis auch vergleichsweise gering. Ein schematischer Aufbau ist in Abbildung 1.1 dargestellt.

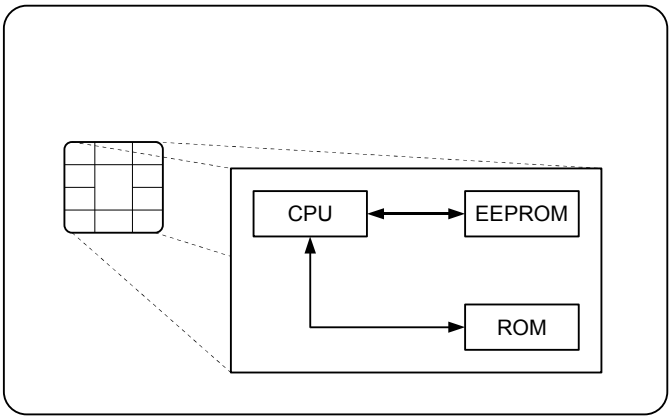

Fig. 1.1: Prinzipieller Aufbau einer Speicherkarte

BER-TLV

Die BER-TLV-Codierung (engl. basic encoding rule) wurde in der Norm ITU-T Rec. X.690 (siehe [ITU97]) definiert und wird vom Standard ISO/IEC 7816-4 in leicht eingeschränkter Form übernommen. Aufgrund der geringen Speicherfähigkeit von Chipkarten wurde das maximale Fassungsvermögen dieser Datenobjekte auf ein praktikables Maß reduziert. Aufgrund der TLV-Struktur besteht ein BER-TLV-Datenobjekt wiederum aus einem Kennzeichen, einer Längenangabe und dem optionalem Nutzdatenteil (siehe Abbildung **??**).

Tag

Die Bezeichnung (siehe Tabelle 1.1) darf nach ISO/IEC 7816-4 eine Länge von ein, zwei oder drei Bytes besitzen. Dem ersten Byte kommt eine spezielle Bedeutung zu. Es ordnet das Datenobjekt (Bit 7 und 8) in eine von vier Klassen ein.

1. °00° bildet die universelle Klasse (engl. universal class)
2. °01° bildet die Applikationsklasse (engl. application class)
3. °10° bildet die kontext-spezifische Klasse (engl. context-specific class)
4. °11° bildet die private Klasse (engl. private class)

Tab. 1.1: Codierung des ersten Kennzeichenbytes nach dem BER-TLV-Schema

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
0	0	-	-	-	-	-	-	universelle Klasse
0	1	-	-	-	-	-	-	Applikationsklasse
1	0	-	-	-	-	-	-	kontext-spezifische Klasse
1	1	-	-	-	-	-	-	private Klasse
-	-	0	-	-	-	-	-	einfach (engl. primitiv)
-	-	1	-	-	-	-	-	zusammengesetzt (engl. constructed)
-	-	-	x	x	x	x	x	einfaches Kennzeichen
-	-	-	1	1	1	1	1	komplexes Kennzeichen

Kein 1.1 ohne 1.2

Keine Leerseiten!

Keine mehrzeiligen Überschriften; das sieht schrecklich aus und lässt sich immer vermeiden!

Keine mehrzeiligen Überschriften

Das sieht schrecklich aus und lässt sich immer vermeiden!

- Leerräume nur am Kapitelende!
- Auch die letzte Seite sollte mindestens zur Hälfte gefüllt sein!

Tipps

In diesem Kapitel haben wir einige Tipps und Richtlinien zusammengestellt, die Sie Im Rahmen Ihrer Arbeit berücksichtigen sollten. Die Ausführungen erheben keinen Anspruch auf Vollständigkeit und Richtigkeit.

Wichtiges zum Ablauf der (Master-)Arbeit

Am Anfang

- Literaturrecherche zum Thema (Bibliothek, Online-Ressourcen, ...)
- Nach Diskussion mit Betreuer
  → Abgabe der Gliederung und Besprechung
  → Präsentation der geplanten Arbeit im Privatissimum
- Sie gehen auf die **mündliche** Masterprüfung zu. Wenn Sie bisher nur wenige mündliche Prüfungen abgelegt haben, dann sollten Sie noch bei ein paar Prüfungen üben, damit es bei der Masterprüfung keine Probleme gibt.
- Hören Sie, wenn möglich, bei anderen Masterprüfungen zu. Dann sind Sie bei Ihrer Masterprüfung nicht von der Atmosphäre überrascht. Zudem können Sie so die für Sie passenden Prüfer leichter bestimmen.

Nach dem ersten Drittel

- Elektronische Abgabe eines aussagekräftigen Probekapitels (20 Seiten Text mit Tabellen, Abbildungen und Referenzen). Hier kann Sie (oder besser den Betreuer) ein Probedruck vor bösen Überraschungen (z.B. unleserliche Schriften, schwarze Blöcke in Abbildungen) bewahren.
- Sie erhalten das Probekapitel nach 7-10 Tagen mit Anmerkungen zurück.

Nach der Hälfte (oder zumindest 1 Mal pro Semester)

- Präsentation des aktuellen Standes der Arbeit (1 Teilthema vertiefen) im Privatissimum
- Überprüfen, ob alle nötigen Zeugnisse und Bescheinigungen vorliegen und ob der 3. Abschnitt eingereicht ist.

Spätestens 10 Wochen vor der Masterprüfung

10 Wochen stellen das absolute Minimum dar!

- Elektronische Abgabe der Beta-Version → Sie erhalten die Beta-Version nach 7-10 Tagen mit Kommentaren zurück.
- Präsentation der gesamten Arbeit im Privatissimum.

Spätestens 5 Wochen vor der Masterprüfung

- Abgabe einer CD mit allen Sourcen (*.doc, *.tex, *.ppt, *.vsd, ...) und verwendeter Webseiten beim Betreuer.
- Abgabe der gebundenen Arbeit und aller Unterlagen in der Studienabteilung.
- Was Sie vor dem Binden beachten sollten ...
  - Variable "FINAL" in der Datei "thesis.tex" auf true setzen.
  - Dokument auf nicht aufgelöste Referenzen überprüfen (LaTeX → [?]).
  - Überprüfen Sie die in Word und anderen Editoren markierten Wörter auf richtige Schreibweise.
  - Lassen Sie die Arbeit zudem auf TipPfehler, ortogravische Stillblüten und Wortwiederholungen (jeder hat bestimmte Lieblingswörter) überprüfen – fachfremde Personen lesen meist gründlicher.
  - Umbrüche kontrollieren (einzelne Zeilen/Wörter am Seitenanfang und Seitenende vermeiden).
  - Bei externen Masterarbeiten ist eine aussagekräftige Stellungnahme des externen Betreuers zum fachlichen Inhalt erforderlich.
  - Denken Sie an ein zusätzliches gebundenes Exemplar für die Vorbegutachterin oder den Vorbegutachter (= betreuender Assistent).

3 Wochen vor Masterprüfung (betrifft Gruppe syssec)

- Abgabe der Beurteilung (= Zeugnis)
- Abgabe des Gutachtens (= ausführliche schriftliche Stellungnahme)

Endlich: Der Vortrag bei der Masterprüfung (oder Endpräsentation)

- Wie würden Sie Ihre Masterarbeit mit zwei (bis drei) Sätzen beschreiben?
- Worauf sind Sie besonders stolz?
- Kürzer Überblick, damit alle Anwesenden wissen, was Sie geleistet haben.
- Ein (zwei) Themen herausgreifen und vertieft erläutern, damit Sie einerseits "glänzen" können und die Anwesenden möglicherweise etwas Neues lernen.

Einige Links (Stand 02-2008)

- uni-klu → Index → Termine für das Studienjahr
- Studienabteilung → Formulare → Bachelorarbeit und Masterarbeit
- Studienabteilung → Termine (`http://www.uni-klu.ac.at/studabt/inhalt/431.htm`)

- Studienabteilung → Wissenschaftliche Arbeiten (`http://www.uni-klu.ac.at/studabt/inhalt/1765.htm`)

Diverses

- Unterlagen vor Abgabe in der Studienabteilung kopieren.
- Mit Ablegen der Masterprüfung verlieren Sie den Status "Studierende(r)" und können somit gegebenenfalls auf Sammelzeugnisse oder ähnliche Daten nicht mehr zugreifen. Diese Daten sollten Sie vor der Masterprüfung ausdrucken bzw. als PDF speichern.
- Eventuell im letzten Semester ein Zweitstudium inskribieren, damit man wenigstens noch eingeschränkten Zugang auf seine Daten hat.

Wichtiges zu Bakkalaureatsarbeiten

- Eine Bakkalaureatsarbeit muss vor Beginn als solche deklariert und angemeldet werden.
- Abstract: 170-250 Worte
- Umfang: 8000 Worte
- Sprache: vorzugsweise Deutsch (Englisch nur nach Rücksprache mit dem Betreuer)

Wichtiges zu Seminararbeiten

- Abstract: 170-250 Worte
- Umfang: 5000 Worte
- Sprache: vorzugsweise Deutsch (Englisch nur nach Rücksprache mit dem Betreuer)

Richtlinien und Tipps für wissenschaftliche Arbeiten

Äußere Form

- Die Masterarbeit wird bei Ihren zukünftigen Bewerbungen ein wesentliches Kriterium sein. Der erste Eindruck, den Ihre Arbeit hinterlässt wird immer ein optischer sein! Neben den inhaltlichen Aspekten sollten Sie daher auch auf das äußere Erscheinungsbild Ihrer Arbeit Wert legen.
- Formatierung und Daten der Titelseite und "Ehrenwörtliche Erklärung" laut aktuellen Vorschriften der Studienabteilung!
- Wird die Variable "FEMALE" auf true gesetzt, so werden die Bezeichner "Autorin" und "Diplom-Ingenieurin" auf der Titelseite verwendet. Ist "FEMALE" false, dann werden "Autor" und "Diplom-Ingenieur" verwendet.
- Schrift 11pt Times New Roman, Zeilenabstand 110%, Blocksatz mit Silbentrennung.
- Seitengröße DIN-A4, Ränder r/l/o/u = 2,5/3,0/2,5/2,5 cm
- Doppelseitiger Druck (Kopfzeilen beachten), Kapitelbeginn auf ungerader (rechter) Seite:
  - linke Seite: Seiten-Nr Kapitelname

  - rechte Seite: Abschnittsname Seiten-Nr

- Umfang der Arbeit nach Vereinbarung (Qualität geht vor Quantität). Es gelten jedoch folgende Richtwerte:
  - Masterarbeit: ± 110 Seiten
  - Bakkalaureatsarbeit: ± 8000 Worte
  - Bericht (SWP/WFP): ± 30 Seiten
  - Seminararbeit: ± 5000 Worte
- Sprache nach Vereinbarung – A good German is much better than a bad English. Die Sprachumstellung erfolgt über die boolesche Variable "ENG" in der Datei "thesis.tex". Zudem ist beim Kommando "documentclass" die Option "english" anzugeben.
- LaTeX oder Word? LaTeX sieht technischer aus und ist auch bei vielen Formeln stabil.

Gliederung

- Numerische Gliederung (max. Tiefe 3 – auch im Inhaltsverzeichnis):
  - 1 Kapitel
  - 1.1 Abschnitt
  - 1.1.1 Unterabschnitt (nicht kürzer als eine halbe Seite)
  - Vierte Gliederungsebene nicht nummerieren und auch nicht im Inhaltsverzeichnis eintragen.
- Verzichten Sie auf Abbildungs-, Tabellen- und sonstige Verzeichnisse. Ein Abkürzungsverzeichnis kann jedoch im Einzelfall sehr hilfreich für den Leser sein. Diese Verzeichnisse immer am Ende der Arbeit platzieren.
- Allgemeiner Aufbau
  - Kapitel 1: Einleitung
  - Abschnitt 1.1: Problemstellung und Ziele
  - Abschnitt 1.2: Bestehende Arbeiten
  - Kapitel 2: Allgemeine Grundlagen
  - Kapitel 3 . . . j-1: Theorieteil (Ihre Arbeit)
  - Kapitel j . . . n-1: Praktischer Teil (Ihre Arbeit)
  - Kapitel n: Schlussfolgerungen, Zusammenfassung und Ausblick

  Sourcecode nur auszugsweise in den Hauptteil der Arbeit aufnehmen. Längere Sourcecode-Fragmente in den Anhang.
- Einzeilige Überschriften und Abbildungstexte
- Nach einer Überschrift kommt Text und nicht die nächste Unterüberschrift
- Keine einzelnen Unterpunkte (wenn es keinen Abschnitt X.2 gibt, dann wird Abschnitt X.1 zu Abschnitt X)

Text

- Neue deutsche Rechtschreibung (ggfs. mit Ausnahmen wie Codierung, Sourcecode, ...)
- Fußnoten nur in Ausnahmefällen verwenden.
- Ein Unterpunkt (mit eigener Überschrift) sollte eine halbe Seite nicht unterschreiten.
- Keine leeren und halbleeren Seiten (ggfs. Abbildungen oder Tabellen verschieben) – nur am Ende von Kapiteln ggf. Teile der letzten Seite (weniger als 50%) freilassen. Andere Gründe für leere Teile einer Seite gibt es nicht.
- Zwischenräume nicht aufblähen, um Seiten zu füllen (LaTeX → \raggedbottom).
- Abkürzungen zumindest beim ersten Auftreten im Text ausschreiben (Ausnahme Überschrift, die aber möglichst keine Abkürzungen enthalten sollten): ABK (Abkürzung) oder Abkürzung (ABK). Im ersten Fall erklärt man eine gebräuchliche Abkürzung, im zweiten kürzt man einen in der Arbeit häufig verwendeten Begriff ab (dies aber eher vermeiden, da es meist die Lesbarkeit stört).
- Auf Unterstreichungen, Einfärben und Sperren von Worten am besten ganz verzichten. Falls überhaupt erforderlich für Hervorhebungen am besten fettere Typen, oder eventuell kursive Schrift verwenden.
- Formalisieren Sie die Arbeit nicht zu sehr, dies reduziert die Lesbarkeit.
- Einzelne Zeilen am Seitenende/Seitenanfang und einzelne Wörter am Absatzende vermeiden.
  Diese sieht (wie oben ersichtlich) nicht sehr schön aus.

Abbildungen und Tabellen

- Maximale Breite für Abbildungen festlegen (i.A. wird das die Textbreite sein) und Abbildungen beim Einbetten nicht skalieren.
- Abbildungen selber zeichnen (vorzugsweise Visio - eine Vorlage finden Sie im Ordner "figures") und nicht scannen. Screenshots sind ebenfalls nur in Ausnahmefällen zulässig.
- Abbildungen nicht einfach abzeichnen, sondern überlegen, ob die ganze im Original enthaltenen Information in Ihrer Arbeit sinnvoll ist.
- Gleiches Layout für alle Abbildungen z.B. Blockgröße, Liniendicke, Pfeile und Schriftart (Arial nicht kleiner als 9 pt).
- Farben sind meist nicht notwendig. Wenn doch, dann möglichst sparsam einsetzen.
- Verwenden Sie nach Möglichkeit nur Bilder mit Graustufen. Berücksichtigen Sie insbesondere, dass Bezüge auf farbige Elemente gegebenenfalls ihre Aussage verlieren. So ist die Aussage "In Abbildung 2.1 markiert der rote Pfeil den Fehler." in der linken Hälfte hilfreich, in der rechten nicht.
- Vermeiden Sie in Ihrem Bild zu kleine Schriften (nach Möglichkeit nicht kleiner als 10 pt), Grau- und Farbverläufe. Testen Sie anhand eines Ausdrucks, ob Ihre Graphik gut erkennbar ist.
- Referenzen im Text (z.B. "vgl. Abbildung 1" oder "Tabelle 1 zeigt ...") auf Abbildungen und Tabellen.

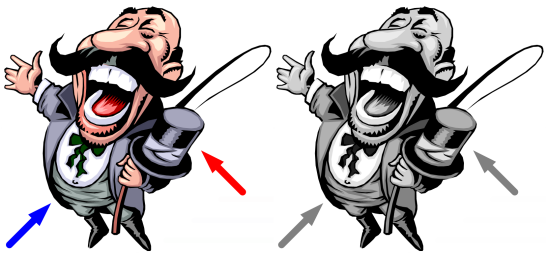

Fig. 2.1: Vorsicht: Auch Cliparts verlieren im SW-Druck ihre Farbe!

- Abbildungen und Tabellen nicht zu weit vom beschreibenden Text platzieren.
- Keine Abbildung (Protokoll, ...) ohne textuelle Beschreibung.
- Keine Seiten, die nur Abbildungen enthalten (LaTeX → textfraction auf 0.05 setzen).
- Abbildungen als eps oder PDF einbinden, NICHT jpg. In Ausnahmefällen können auch PNGs (oder ähnliche verlustlose oder Formate) mit einer Auflösung von mindestens 300 dpi verwendet werden.
- Vektorgrafiken als Basis für die PDF- oder eps-Erstellung nutzen, NICHT jpg.
- Vermeiden Sie Seiten ohne Text, die nur Abbildungen oder Tabellen enthalten.

Formeln

- Quantoren zwecks besserer Lesbarkeit ausschreiben: $\forall \rightarrow$ “für alle”, $\exists \rightarrow$ “es existiert”.
- Logische Verknüpfungen zwecks besserer Lesbarkeit ausschreiben: $\wedge \rightarrow$ “und”, $\vee \rightarrow$ “oder”.
- Text in Formeln nicht kursiv.
- Möglichst keine Nummerierung der Formeln (außer man bezieht sich im Text darauf).
- Kurze aussagekräftige Bezeichner für Funktionen verwenden; z.B.: $\mathrm{encrypt}(m,k) \rightarrow \mathrm{E}(m,k)$ oder $\mathrm{E}_k(m)$, $\mathrm{decrypt}(c,k) \rightarrow \mathrm{D}(c,k)$ oder $\mathrm{D}_k(c)$, $\mathrm{sign}(m,(d,n)) \rightarrow \mathrm{S}(m,d)$, $\mathrm{verify}(m,s,(e,n)) \rightarrow \mathrm{V}(m,s,e)$, $\mathrm{hash}(m) \rightarrow \mathrm{H}(m)$, ...

Diverses

- Nicht trennbare Leerzeichen zwischen Maßzahl und Einheit einfügen → in LaTeX z.B. ‘3~m’, in Word erzeugt die Tastenkombination ‘Strg+Shift+SPACE’ nicht trennbare Leerzeichen (diese wird dann beispielsweise als ‘3°m’ angezeigt).
- Leerzeichen zwischen z.B. und Text.
- Description-Umgebung mit ‘:’ → LaTeX: \item[<**Text**>**:**] <Text>
- Die Einheiten Bit/Byte immer groß schreiben, dafür ohne Mehrzahl.
- Abkürzung des MAC (Message Authentication Code) nur in der Mehrzahl mit ‘s’.

Ausdruck und Stil

- Allgemein gilt, dass es mit kurzen Sätzen besser gelingt, klare Aussagen zu machen.
- Verzichten Sie auf “blumige Ausdrucksweise” und (allzu) persönliche Stellungnahmen in der “Ich-Form”.

- Die “Ich-” und “Wir-” Form sind zumeist unangebracht: Die Ich-Form betont unnötig die Subjektivität des Gesagten, die Wir-Form erinnert an den Pluralis majestatis.
- Wörter wie “sehr”, “äußerst”, “höchst”, “immens”, “ungeheuer”, “durchaus”, “selbstverständlich”, “natürlich”, “zweifellos” und ähnliche nutzen sich schnell ab und sind äußerst sparsam zu verwenden.
- Ausdrücke wie “eigentlich”, “im Grunde genommen”, “irgendwie”, “an und für sich”, “gewissermaßen” enthüllen oft, was dem Verfasser zweifelhaft vorkommt: Er sollte dies direkt sagen.
- Offene Wertungen, wie Sätze mit “leider”, “erfreulicherweise”, “glücklicherweise”, sind zu vermeiden.
- Formulierungen wie “. . . soll zeigen, dass . . . ” vermeiden → “. . . zeigt, dass . . . ” klingt überzeugter.
- Wortwiederholungen sind zu vermeiden.
- Fachausdrücke und Fremdwörter sind mit Sorgfalt zu verwenden, ungebräuchliche oder selbst definierte Abkürzungen zu vermeiden.
- Nicht jeder englische Fachausdruck kann prägnant übersetzt werden. In manchen Fällen gibt es keinen deutschen Ausdruck.
- Ausrufezeichen ‘!’ sparsam einsetzen!!! In der Masterarbeit stehen ohnedies nur wichtige Dinge!!!

Zitierrichtlinien

- Auch wir kennen ein paar Bücher und zudem können wir googeln!
- Nutzen Sie die Möglichkeiten und Veranstaltungen des SchreibCenters der Universität Klagenfurt (`http://www.uni-klu.ac.at/uniklu/org/oe.jsp?orgkey=706`)
- “Korrektes wissenschaftliches Arbeiten bedeutet, dass jede Verwendung fremden geistigen Eigentums (Gedanken, Argumentationen, Daten und Informationen) durch eine genaue Quellenangabe kenntlich zu machen ist. Das soll dem Leser der Arbeit die Feststellung ermöglichen, ob die vorgetragenen Gedanken vom Verfasser oder von fremder Herkunft sind. Durch exaktes Zitieren kann der Entstehungsprozess von wissenschaftlichen Aussagen zurückverfolgt werden. Außerdem wird die weitere Recherche für am Thema Interessierte ermöglicht.” (vgl. DA-Richtlinien der WU-Wien [WUWi01])
- Wörtlich übernommene Passagen sind zu vermeiden oder so kurz wie möglich zu halten.
- Falls Textpassagen doch wörtlich übernommene werden, so sind sie unter Anführungszeichen zu setzen. Die Auslassung von Wörtern ist durch drei Punkte zu kennzeichnen.
- Auch die sinngemäße Wiedergabe fremden geistigen Eigentums ist durch genaue Quellenangabe kenntlich zu machen (siehe [NNNN00]).

Literatur

- Bibstyle Alpha: 4 Buchstaben für den/die Nachnamen und zwei Ziffern für das Jahr (NNNNYY, NaNNYY, NaNaYY, NameYY). Bei mehreren Publikationen im selben Jahr:

NNNYYa, NNNYYb, ..., sinnvolle Ausnahmen (z.B. bei Standards) sind erlaubt, da sie die Lesbarkeit erhöhen.
LaTeX:

  - Alle Literatureinträge gleich weit einrücken (ggfs. \begin{thebibliography}{<breiteste Abkürzung>} nutzen.
  - Datei *.bbl gegebenenfalls vor dem letzten Durchlauf händisch an NNNNYY anpassen (und in Kopie speichern).

- Graue Literatur (z.B. LV-Unterlagen, Master/Diplom- oder Seminararbeiten) vermeiden. Es gibt immer Bücher oder wissenschaftliche Papers zur selben Thematik!
- Wikis sind gute Ausgangspunkte für Recherchen, haben im Literaturverzeichnis aber nichts verloren.
- Referenzen auf Webseiten nur dann anführen, wenn es zu der entsprechenden Thematik kein Buch oder wissenschaftliches Paper gibt! Verwendete Inhalte aus dem Web für den Fall, dass sie später nicht mehr verfügbar sind, jedenfalls lokal sichern.

Implementierungen

GET CHALLENGE

Der Quellcode A.1 enthält den Code der `GetChallengeHandler`-Klasse ohne Kommentare. Durch platzsparendes Einrücken konnte ein ungünstiger Seitenumbruch vermieden werden.

```
package at.ac.uniklu.simulator.commands.iso7816;

import java.util.Random;

import at.ac.uniklu.simulator.commands.CommandHandler;
import at.ac.uniklu.simulator.commands.CommandPattern;
import at.ac.uniklu.simulator.commands.ISO7816DefaultReturnCodes;
import at.ac.uniklu.simulator.commands.RAPDU;
import at.ac.uniklu.simulator.util.Enum1;
import at.ac.uniklu.simulator.util.HEXByteString;

public class GetChallengeHandler extends CommandHandler
{
  public String getIdentifier()
  {
    return "GetChallenge";
  }

  public CommandPattern getCommandPattern()
  {
    return new CommandPattern("XX", "84");
  }

  protected Enum1 returnDataStatus()
  {
    return EnumStatus.needed;
  }

  public Enum1 dataStatus()
  {
    return EnumStatus.notallowed;
  }

  public RAPDU preExecute()
  {
    RAPDU ret = super.preExecute();
    if (ret != null)
      return ret;

    if (command.getP1().getByte() != 0 || command.getP2().getByte() != 0)
      return ISO7816DefaultReturnCodes.get(ISO7816DefaultReturnCodes.codes.SW_WRONG_PARAMETERS);
    return null;
  }
```

```
  public RAPDU execute()
  {
    Random r = new Random();
    int randnum = command.getNe();

    byte[] rbytes = new byte[randnum];
    r.nextBytes(rbytes);

    RAPDU ret = ISO7816DefaultReturnCodes.get(ISO7816DefaultReturnCodes.codes.SW_NO_ERROR);
    ret.setData(new HEXByteString(rbytes));

    this.getOpSys().getCurrentSession().setChallenge(new HEXByteString(rbytes));

    return ret;
  }
}
```

Src. A.1: Implementierung des GET CHALLENGE Kommandos

Kein A.1 ohne A.2

Bibliography

[Ashb00] J. D. M. Ashbourn: Biometrics : Advanced Identify Verification: The Complete Guide. Springer Verlag (2000).

[BeKH01] K. Beuth, G. Kurz, R. Hanebuth: Nachrichtentechnik. Vogel Fachbuch, Vogel-Verlag KG., Würzburg (2001).

[BeKP91] A. Beutelspacher, A. G. Kersten, A. Pfau: Chipkarten als Sicherheitswerkzeug. Springer Verlag, Berlin (1991).

[BiSh91] E. Biham, A. Shamir: Differential Cryptanalysis of DES-like Cryptosystems. *In: CRYPTO '90: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag, London, UK (1991), 2–21.

[Breu84] R. Breuer: Computer-Schutz durch Sicherung und Versicherung. Karamanolis-Verlag (1984).

[Chen00] Z. Chen: Java Card Technology for Smart Cards: Architecture and Programmer's Guide (The Java Series). Addison-Wesley (2000).

[DaRi00] J. Daemen, V. Rijmen: The Block Cipher Rijndael. *In: CARDIS '98: Proceedings of the The International Conference on Smart Card Research and Applications*, Springer-Verlag, London, UK (2000), 277–284.

[ITU97] International Telecommunication Union: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER),Canonical Encoding Rules (CER) and Distinguished Encoding Rules(DER) (1997), `http://www.itu.int`, iTU-T Rec. X.690 (2002) — ISO/IEC 8825-1:2002.

[JoMV01] D. Johnson, A. Menezes, S. A. Vanstone: The Elliptic Curve Digital Signature Algorithm (ECDSA). In: *International Journal on Information Security*, 1, 1 (2001), 36–63.

[MeVO96] A. J. Menezes, S. A. Vanstone, P. C. V. Oorschot: Handbook of Applied Cryptography. CRC Press, Inc., Boca Raton, FL, USA (1996).

[NIST77] NIST: Data Encryption Standard, *Federal information processing standards publication*, Bd. 46. National Institute for Standards and Technology (1977).

[NIST00] NIST: FIPS PUB 186-2 Digital Signature Standard (DSS). National Institute for Standards and Technology, Gaithersburg, MD, USA (2000), `http://www.itl.nist.gov/fipspubs/fip186-2.pdf`.

[RaEf02] W. Rankl, W. Effing: Handbuch der Chipkarten. Carl Hanser Verlag München Wien (2002), 4., überarbeitete und aktualisierte Auflage.

[Rank06] W. Rankl: Chipkartenanwendungen. Carl Hanser Verlag München Wien (2006), entwurfsmuster für Einsatz und Programmierung von Chipkarten.

[RiSA78] R. L. Rivest, A. Shamir, L. M. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. In: *Communications of the ACM*, 21, 2 (1978), 120–126.