RKSV (technisch) v6.3

Ramin Sabet, Patrick Hagelkruys

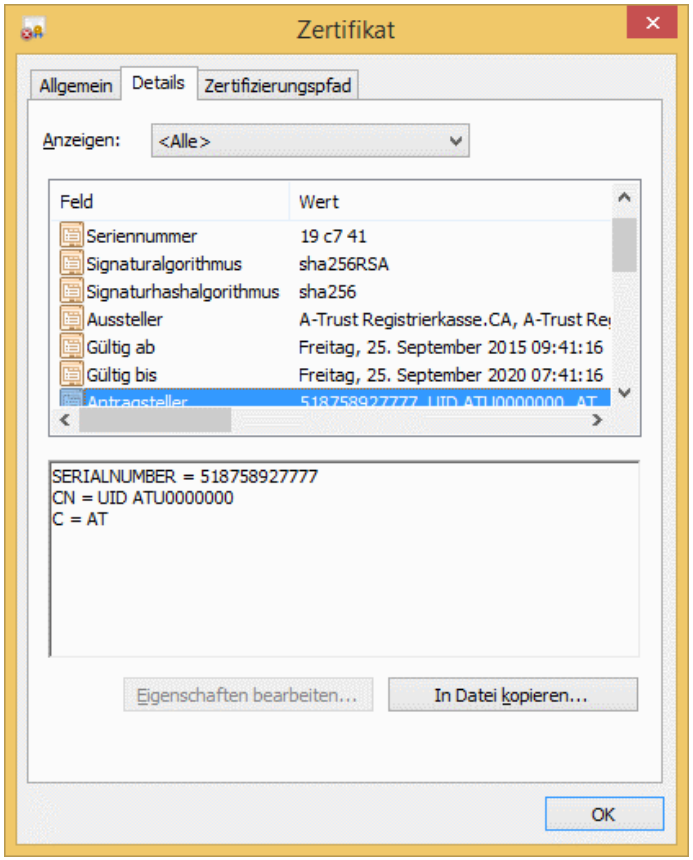
A-Trust GmbH

2016-12-01

Agenda

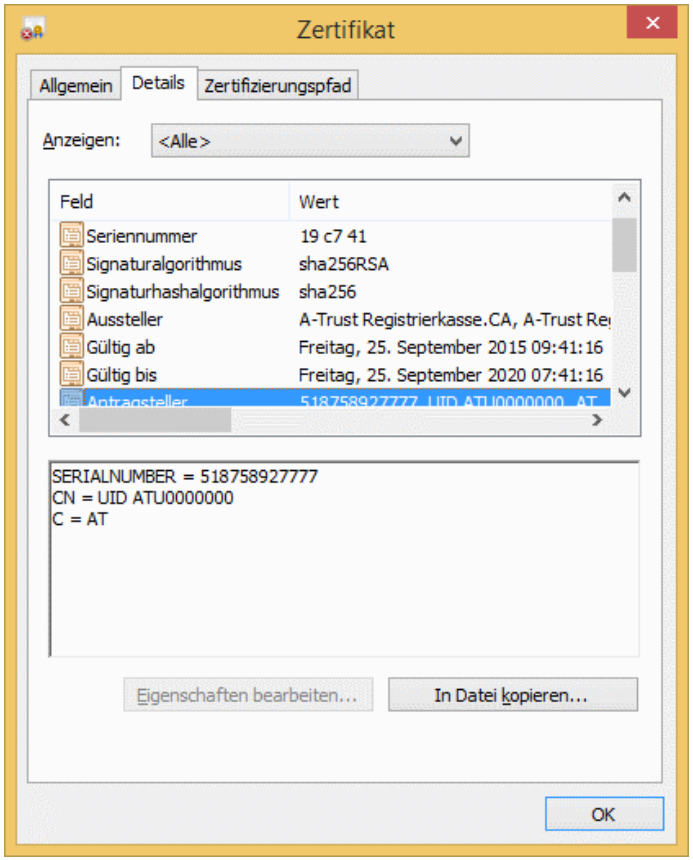
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



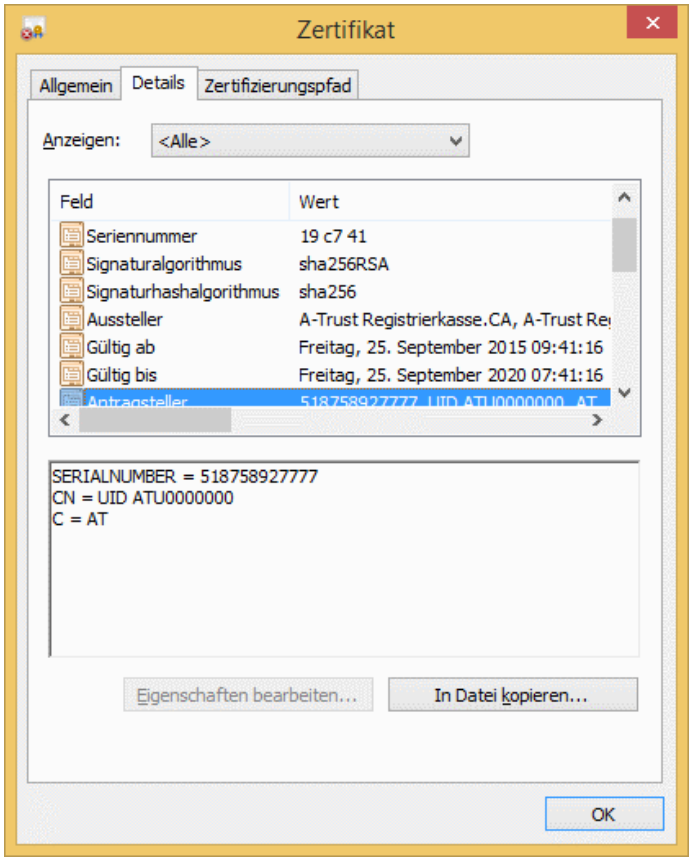
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



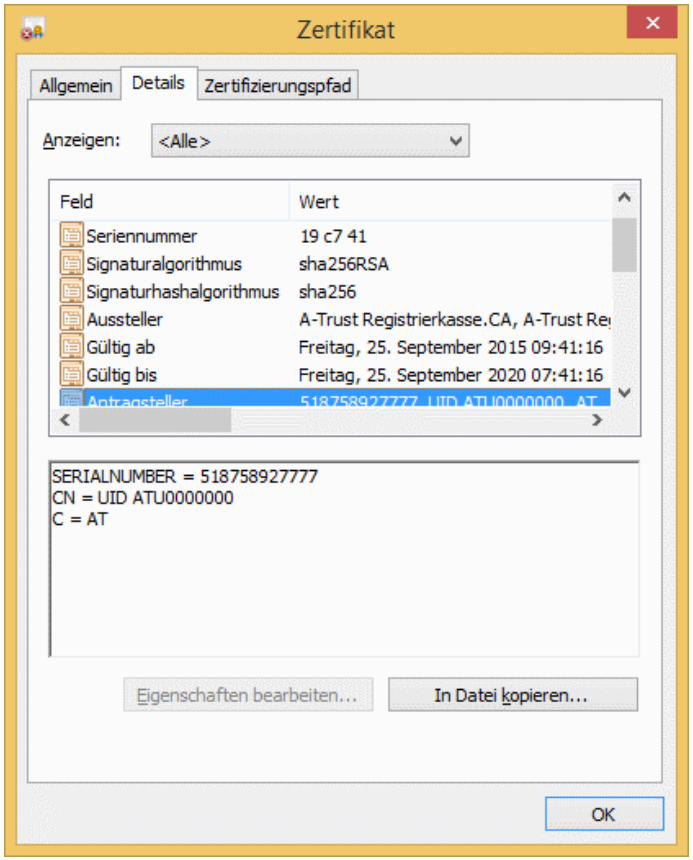
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



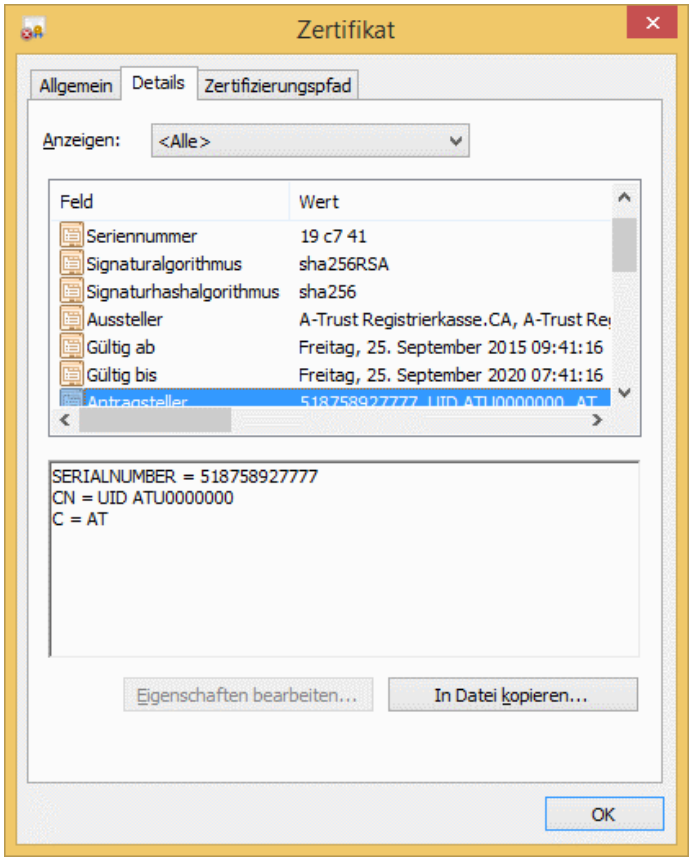
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



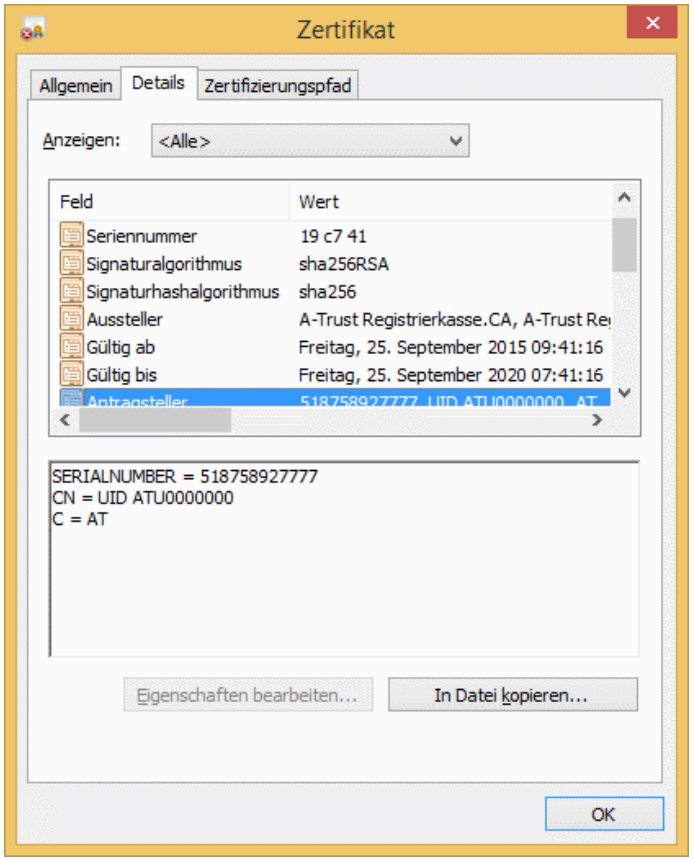
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



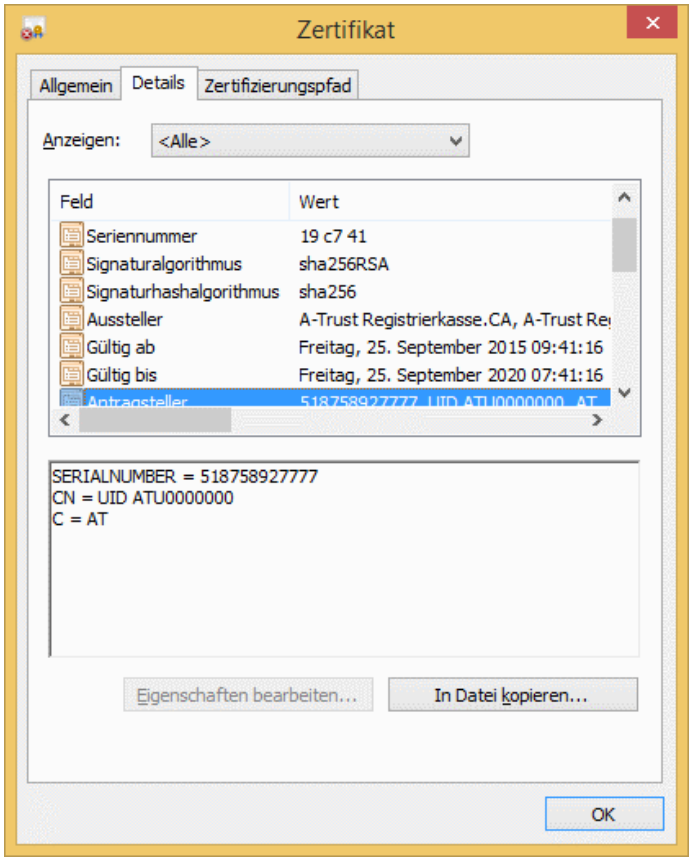
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



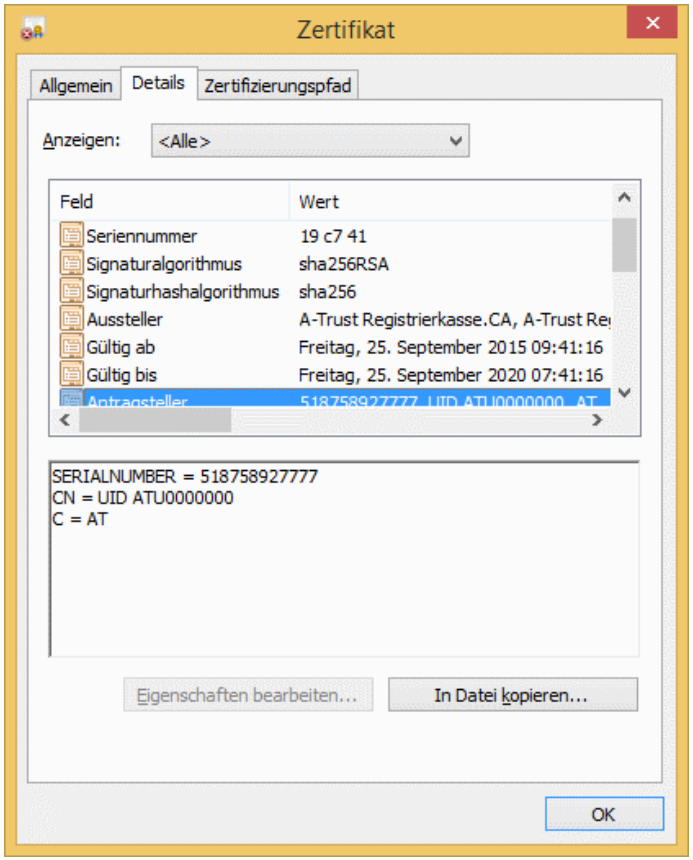
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



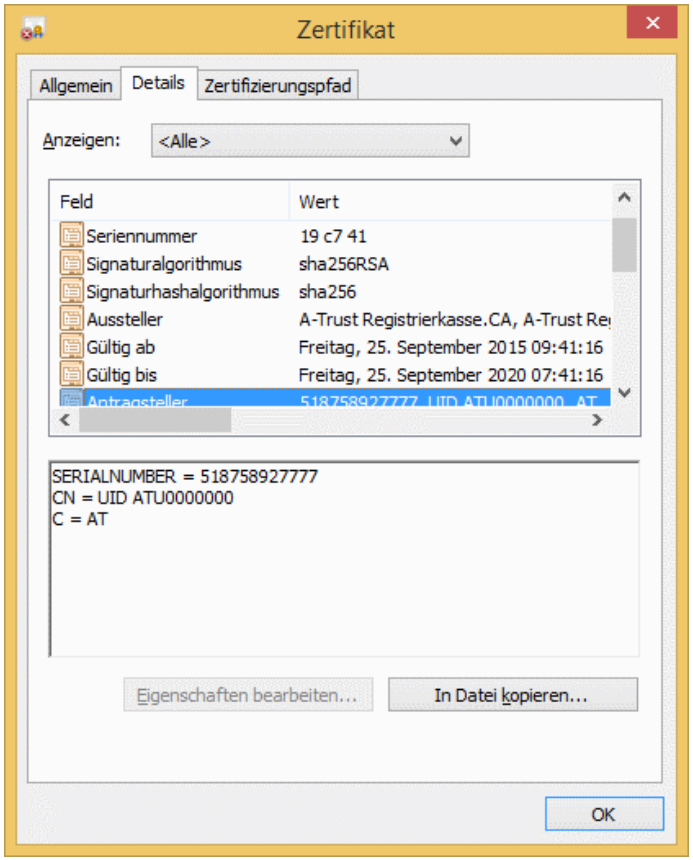
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



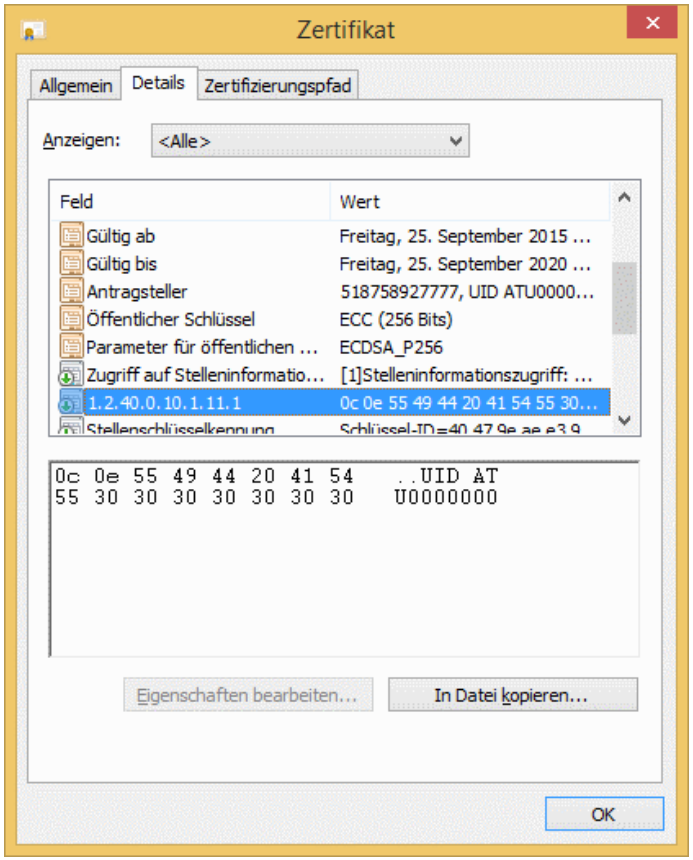
a.sign RK CHIP

- EUR 9
- Karte
- 2 Schlüsselpaare
  - PIN: 123456
- Zertifikat
  - Qualifiziert? Nein
  - Seriennummer
  - Gültigkeit
- Kartenleser



a.sign RK ONLINE

- OID
- Je Ordnungsbegriff ein Zertifikat
- Mehrere Zertifikate je Kasse möglich
- Mehrere Kassen mit gleichem Ordnungsbegriff können sich Zertifikat teilen



a.sign RK ONLINE

- EUR 4
- Shared Hardware Security Module
- Privater Schlüssel im A-Trust Rechenzentrum (HSM)
- online Verbindung
- Wenn ich selbst ein HSM habe . . .

a.sign RK ONLINE

- EUR 4
- Shared Hardware Security Module
- Privater Schlüssel im A-Trust Rechenzentrum (HSM)
- online Verbindung
- Wenn ich selbst ein HSM habe . . .

a.sign RK ONLINE

- EUR 4
- Shared Hardware Security Module
- Privater Schlüssel im A-Trust Rechenzentrum (HSM)
- online Verbindung
- Wenn ich selbst ein HSM habe . . .

a.sign RK ONLINE

- EUR 4
- Shared Hardware Security Module
- Privater Schlüssel im A-Trust Rechenzentrum (HSM)
- online Verbindung
- Wenn ich selbst ein HSM habe . . .

a.sign RK ONLINE

- EUR 4
- Shared Hardware Security Module
- Privater Schlüssel im A-Trust Rechenzentrum (HSM)
- online Verbindung
- Wenn ich selbst ein HSM habe ...

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

a.sign RK HSM

- HSM exklusiv für einen Kunden
- ansprechbar über REST (vergleichbar RK Online)
- Vorteil:
  - geeignet für hohes Volumen an Signaturen
  - höchste Performance
  - keine Internetverbindung
  - kein USB
  - redundanz möglich

Welche Lösung für wen

- Online: wenn nicht zeitkritisch, oder kein USB möglich
- Chip: wenige Kassen, kein Internet
- HSM: alle Vorteile
- Testsystem: `http://labs.a-trust.at/developer/pdf/RegistrierkasseMobileDev.pdf`

Welche Lösung für wen

- Online: wenn nicht zeitkritisch, oder kein USB möglich
- Chip: wenige Kassen, kein Internet
- HSM: alle Vorteile
- Testsystem: `http://labs.a-trust.at/developer/pdf/RegistrierkasseMobileDev.pdf`

Welche Lösung für wen

- Online: wenn nicht zeitkritisch, oder kein USB möglich
- Chip: wenige Kassen, kein Internet
- HSM: alle Vorteile
- Testsystem: http://labs.a-trust.at/developer/pdf/RegistrierkasseMobileDev.pdf

Welche Lösung für wen

- Online: wenn nicht zeitkritisch, oder kein USB möglich
- Chip: wenige Kassen, kein Internet
- HSM: alle Vorteile
- Testsystem: http://labs.a-trust.at/developer/pdf/RegistrierkasseMobileDev.pdf

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Ausstellung

- Wer kann Zertifikat ausstellen
- Registration Officer (spezielle Berechtigung)
  - Nicht notwendig
- SSL Verbindung
- Was muss angegeben werden
  - Ordnungsbegriff: einer der folgenden Werte:
    - UID
    - GLN
    - Steuernummer
  - Email (für Informationen, z.B.: Ablauf)

Chip

- Bestellung: aktivierbare Karten im A-Trust Webshop
- DEMO - Ausstellung

Online

- Guthaben im A-Trust Webshop
  - Login zur Ausstell-Plattform
  - REST-Interface
    - ZDA-Info
    - Certificate, CertChain, CertSerialNr
- Transaktions History

Agenda

a.sign RK CHIP - APDU

- APDU (Application Protocol Data Unit)

```
String PIN = "123456";
[...]
CommandAPDU command = new CommandAPDU(0x00, 0xA4, 0x04, 0x00, APPLICATION_ID, 256);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x22, 0x41, 0xb6, TLV);
executeCommand(channel, command);

command = new CommandAPDU(format(0x00, 0x20, 0x00, 0x81, 0x08, PIN));

executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x90, 0x81, sha256Hash);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x9E, 0x9A, 256);
byte[] sig = getData(channel, command);
```

- Kartenlesertreiber
- Keine weitere Software notwendig
- Weitere Sprachen, aktuelle Version: labs.a-trust.at

a.sign RK CHIP - APDU

- APDU (Application Protocol Data Unit)

```
String PIN = "123456";
[...]
CommandAPDU command = new CommandAPDU(0x00, 0xA4, 0x04, 0x00, APPLICATION_ID, 256);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x22, 0x41, 0xb6, TLV);
executeCommand(channel, command);

command = new CommandAPDU(format(0x00, 0x20, 0x00, 0x81, 0x08, PIN));

executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x90, 0x81, sha256Hash);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x9E, 0x9A, 256);
byte[] sig = getData(channel, command);
```

- Kartenlesertreiber
- Keine weitere Software notwendig
- Weitere Sprachen, aktuelle Version: labs.a-trust.at

a.sign RK CHIP - APDU

- APDU (Application Protocol Data Unit)

```
String PIN = "123456";
[...]
CommandAPDU command = new CommandAPDU(0x00, 0xA4, 0x04, 0x00, APPLICATION_ID, 256);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x22, 0x41, 0xb6, TLV);
executeCommand(channel, command);

command = new CommandAPDU(format(0x00, 0x20, 0x00, 0x81, 0x08, PIN));

executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x90, 0x81, sha256Hash);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x9E, 0x9A, 256);
byte[] sig = getData(channel, command);
```

- Kartenlesertreiber
- Keine weitere Software notwendig
- Weitere Sprachen, aktuelle Version: labs.a-trust.at

a.sign RK CHIP - APDU

- APDU (Application Protocol Data Unit)

```
String PIN = "123456";
[...]
CommandAPDU command = new CommandAPDU(0x00, 0xA4, 0x04, 0x00, APPLICATION_ID, 256);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x22, 0x41, 0xb6, TLV);
executeCommand(channel, command);

command = new CommandAPDU(format(0x00, 0x20, 0x00, 0x81, 0x08, PIN));

executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x90, 0x81, sha256Hash);
executeCommand(channel, command);
command = new CommandAPDU(0x00, 0x2A, 0x9E, 0x9A, 256);
byte[] sig = getData(channel, command);
```

- Kartenlesertreiber
- Keine weitere Software notwendig
- Weitere Sprachen, aktuelle Version: labs.a-trust.at

a.sign RK CHIP - a.sign Client

- a.sign Client (labs.a-trust.at)

```
CK_DEFINE_FUNCTION(CK_RV, C_RKInfo)(
    CK_UTF8CHAR ZdaId[3],
    CK_BYTE_PTR pSigCertSerial,
    CK_ULONG_PTR pulSigCertSerialLen,
    CK_BYTE_PTR pSigCert,
    CK_ULONG_PTR pulSigCertLen,
    CK_BYTE_PTR pIssuerCert,
    CK_ULONG_PTR pulIssuerCertLen
);

CK_DEFINE_FUNCTION(CK_RV, C_RKSign)(
    CK_BYTE_PTR pData,
    CK_ULONG ulData,
    CK_BYTE_PTR pSignature,
    CK_ULONG_PTR pulSignatureLen
);
```

a.sign RK ONLINE, HSM

REST Interface zur einfachen Nutzung

- Sign

```
POST /asignrkonline/v2/{Benutzername}/Sign/JWS HTTP/1.1
Content-Type: application/json
Host: ...
Content-Length: 247

{
"password":"123456789",
"jws_payload":"_R1-AT0_DEMO-C...oRo="
}
```

- Antwort

```
HTTP/1.1 200 OK
Content-Length: 189
Content-Type: application/json; charset=utf-8

{
"result":"ey...J9.X1I...z0=.an...Q==",
}
```

a.sign RK ONLINE, HSM

- Zertifikatsinformationen

```
GET /asignrkonline/v2/{Benutzername}/Certificate HTTP/1.1
```

- Antwort

```
HTTP/1.1 200 OK
Content-Length: 1540
Content-Type: application/json; charset=utf-8

{
"Signaturzertifikat":"MIIE...QA6o=",
"Zertifizierungsstellen":["MII...WSF"],
"Zertifikatsseriennummer":"963244432",
"ZertifikatsseriennummerHex":"3969F190",
"alg":"ES256"
}
```

a.sign RK ONLINE, HSM: ZDA-Info

- ZDA-Informationen abfragen

```
GET /asignrkonline/v2/{Benutzername}/ZDA HTTP/1.1
```

- Antwort

```
HTTP/1.1 200 OK
Content-Length: 15
Content-Type: application/json; charset=utf-8

{
"zdaid":"AT1"
}
```

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Unterstützte Betriebssysteme

- Online, HSM
  - alle
- APDU (Bei Karten-OS Änderung Anpassung notwendig)
  - alle
- a.sign Client
  - Windows (Setup oder copy-install)
  - Linux (getestet: debian, suse, raspberry)

Agenda

Ressourcen

- BMF: RKSV
- A-SIT Plus begleitet das RKSV Projekt
- Demo Code: a-sit Plus
- github Projekt: github
- FinanzOnline: Webservice FON
  - Registrierkasse anmelden
  - Registrierkasse abmelden
  - Registrierkasse ausgefallen
- WKO Registrierkassenpflicht
  - Informationen zur Kassen- und Belegerteilungspflicht 2016/2017
  - englische Übersetzung
  - Video-Tutorial Registrierkassen-Anmeldung bei FinanzOnline Video-Tutorial

Signaturformat

- RKSV/Anlage/Detailspezifikation/Z5/Signaturformat

  `Wert(Kassen-ID)_Wert(Belegnummer)_Wert(Beleg-Datum-Uhrzeit)_`
  `Wert(Betrag-Satz-Normal)_Wert(Betrag-Satz-Ermaessigt-1)_Wert(Betrag-Satz-Ermaessigt-2)_Wert(Betrag-Satz-Null)_Wert(Betrag-Satz-Besonders)_`
  `Wert(Stand-Umsatz-Zaehler-AES256-ICM)_Wert(Zertifikat-Seriennummer)_`
  `Wert(Sig-Voriger-Beleg)`

- Beispiel (qr-code-rep.txt)

```
_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_0gJTFI8/zqc=\
    _D7259417A07DFB1_fP7/PMPSnQ0=_Xh5wNe0akaTOVvMgLVrCcR [...]
_R1-AT1_DEMO-CASH-BOX426_776731_2015-10-14T18:20:23_5,41_0,00_0,00_0,00_0,00_E/UH4GsbdK4=\
    _D7259417A07DFB1_vfncd0LgJuE=_jCuMXa0c0sTXvMy8T9yoJ [...]
```

- ZDA-Info (hier: AT1) info: online, client
- Zertifikats info: online, client
- Signatur voriger Beleg:

  "Für die Erfassung des ersten Barumsatzes wird der Wert des Felds Kassen-ID als Input dieser Hash-Funktion verwendet"

  sonst `8 bytes(SHA256(vorige Signatur))`

Signaturformat

- RKSV/Anlage/Detailspezifikation/Z5/Signaturformat

  `Wert(Kassen-ID)_Wert(Belegnummer)_Wert(Beleg-Datum-Uhrzeit)_`
  `Wert(Betrag-Satz-Normal)_Wert(Betrag-Satz-Ermaessigt-1)_Wert(Betrag-Satz-Ermaessigt-2)_Wert(Betrag-Satz-Null)_Wert(Betrag-Satz-Besonders)_`
  `Wert(Stand-Umsatz-Zaehler-AES256-ICM)_Wert(Zertifikat-Seriennummer)_`
  `Wert(Sig-Voriger-Beleg)`

- Beispiel (qr-code-rep.txt)

```
_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_0gJTFI8/zqc=\
    _D7259417A07DFB1_fP7/PMPSnQ0=_Xh5wNe0akaTOVvMgLVrCcR [...]
_R1-AT1_DEMO-CASH-BOX426_776731_2015-10-14T18:20:23_5,41_0,00_0,00_0,00_0,00_E/UH4GsbdK4=\
    _D7259417A07DFB1_vfncd0LgJuE=_jCuMXa0c0sTXvMy8T9yoJ [...]
```

- ZDA-Info (hier: AT1) info: online, client
- Zertifikats info: online, client
- Signatur voriger Beleg:

  "Für die Erfassung des ersten Barumsatzes wird der Wert des Felds Kassen-ID als Input dieser Hash-Funktion verwendet"

  sonst `8 bytes(SHA256(vorige Signatur))`

Signaturformat

- RKSV/Anlage/Detailspezifikation/Z5/Signaturformat

  `Wert(Kassen-ID)_Wert(Belegnummer)_Wert(Beleg-Datum-Uhrzeit)_`
  `Wert(Betrag-Satz-Normal)_Wert(Betrag-Satz-Ermaessigt-1)_Wert(Betrag-Satz-Ermaessigt-2)_Wert(Betrag-Satz-Null)_Wert(Betrag-Satz-Besonders)_`
  `Wert(Stand-Umsatz-Zaehler-AES256-ICM)_Wert(Zertifikat-Seriennummer)_`
  `Wert(Sig-Voriger-Beleg)`

- Beispiel (qr-code-rep.txt)

```
_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_0gJTFI8/zqc=\
    _D7259417A07DFB1_fP7/PMPSnQ0=_Xh5wNe0akaT0VvMgLVrCcR [...]
_R1-AT1_DEMO-CASH-BOX426_776731_2015-10-14T18:20:23_5,41_0,00_0,00_0,00_0,00_E/UH4GsbdK4=\
    _D7259417A07DFB1_vfncd0LgJuE=_jCuMXa0c0sTXvMy8T9yoJ [...]
```

- ZDA-Info (hier: AT1) info: online, client
- Zertifikats info: online, client
- Signatur voriger Beleg:

  "Für die Erfassung des ersten Barumsatzes wird der Wert des Felds Kassen-ID als Input dieser Hash-Funktion verwendet"

  sonst 8 bytes(SHA256(vorige Signatur))

Signaturformat

- RKSV/Anlage/Detailspezifikation/Z5/Signaturformat

  `Wert(Kassen-ID)_Wert(Belegnummer)_Wert(Beleg-Datum-Uhrzeit)_`
  `Wert(Betrag-Satz-Normal)_Wert(Betrag-Satz-Ermaessigt-1)_Wert(Betrag-Satz-Ermaessigt-2)_Wert(Betrag-Satz-Null)_Wert(Betrag-Satz-Besonders)_`
  `Wert(Stand-Umsatz-Zaehler-AES256-ICM)_Wert(Zertifikat-Seriennummer)_`
  `Wert(Sig-Voriger-Beleg)`

- Beispiel (qr-code-rep.txt)

```
_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_0gJTFI8/zqc=\
    _D7259417A07DFB1_fP7/PMPSnQ0=_Xh5wNe0akaTOVvMgLVrCcR [...]
_R1-AT1_DEMO-CASH-BOX426_776731_2015-10-14T18:20:23_5,41_0,00_0,00_0,00_0,00_E/UH4GsbdK4=\
    _D7259417A07DFB1_vfncd0LgJuE=_jCuMXa0c0sTXvMy8T9yoJ [...]
```

- ZDA-Info (hier: AT1) info: online, client
- Zertifikats info: online, client
- Signatur voriger Beleg:

  "Für die Erfassung des ersten Barumsatzes wird der Wert des Felds Kassen-ID als Input dieser Hash-Funktion verwendet"

  sonst 8 bytes(SHA256(vorige Signatur))

Signaturformat

- RKSV/Anlage/Detailspezifikation/Z5/Signaturformat

  `Wert(Kassen-ID)_Wert(Belegnummer)_Wert(Beleg-Datum-Uhrzeit)_`
  `Wert(Betrag-Satz-Normal)_Wert(Betrag-Satz-Ermaessigt-1)_Wert(Betrag-Satz-Ermaessigt-2)_Wert(Betrag-Satz-Null)_Wert(Betrag-Satz-Besonders)_`
  `Wert(Stand-Umsatz-Zaehler-AES256-ICM)_Wert(Zertifikat-Seriennummer)_`
  `Wert(Sig-Voriger-Beleg)`

- Beispiel (qr-code-rep.txt)

```
_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_0gJTFI8/zqc=\
    _D7259417A07DFB1_fP7/PMPSnQ0=_Xh5wNe0akaTOVvMgLVrCcR [...]
_R1-AT1_DEMO-CASH-BOX426_776731_2015-10-14T18:20:23_5,41_0,00_0,00_0,00_0,00_E/UH4GsbdK4=\
    _D7259417A07DFB1_vfncd0LgJuE=_jCuMXa0c0sTXvMy8T9yoJ [...]
```

- ZDA-Info (hier: AT1) info: online, client
- Zertifikats info: online, client
- Signatur voriger Beleg:
  "Für die Erfassung des ersten Barumsatzes wird der Wert des Felds Kassen-ID als Input dieser Hash-Funktion verwendet"

  sonst `8 bytes(SHA256(vorige Signatur))`

Export Format - Beispiel

- RKSV/Anlage/Detailspezifikation/Z6/Ergebnis der Signaturerstellung
  1. Metainformationen über den verwendeten Hash bzw. Signaturalgorithmus
  2. signierte Daten (JWS Payload) und
  3. berechneter Signaturwert.
- Beispiel


```
{
  "Belege-Gruppe": [
    {
      "Signaturzertifikat": "MIIBSDCB8KADAgECAggNcllBegffsTAKBggqhkjOPQQDAjAWMRQ
      "Zertifizierungsstellen": [
        "MIIBQzCB6aADAgECAgg0UQZRK6AETzAKBggqhkjOPQQDAjAXMRUwEwYDVQQDDAxSZWdLYXN
      ],
      "Belege-kompakt": [
        "eyJhbGciOiJFUzI1NiJ9.X1IxLUFUMF9ERU1PLUNBU0gtQk9YNDI2Xzc3NjczMF8yMDE1LT
        "eyJhbGciOiJFUzI1NiJ9.X1IxLUFUMF9ERU1PLUNBU0gtQk9YNDI2Xzc3NjczMV8yMDE1LT
        "eyJhbGciOiJFUzI1NiJ9.X1IxLUFUMF9ERU1PLUNBU0gtQk9YNDI2Xzc3NjczM18yMDE1LT
        "eyJhbGciOiJFUzI1NiJ9.X1IxLUFUMF9ERU1PLUNBU0gtQk9YNDI2Xzc3NjczM18yMDE1LT
        "eyJhbGciOiJFUzI1NiJ9.X1IxLUFUMF9ERU1PLUNBU0gtQk9YNDI2Xzc3NjczNF8yMDE1LT
      ]
    },
```

Export Format - Details

- Ein Beleg im Detail

  `"eyJhbGciOiJFUzI1NiJ9.X1IxLUFUMF9ERU1PLUNB[...]wPQ.Xh5wNe0akaTOVvMgLVrCcRh2[...]fg"`

- Metainformationen

  `Base64URL('{"alg":"ES256"}') = eyJhbGciOiJFUzI1NiJ9 - !keine Leerzeichen oder Umbrüche!`

  info: online

- Payload

  `Base64URL('_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]') = \`
  `X1IxLUFUMF9ERU1PLUNB[...]`

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:

Festlegungen des BMF

- Maschinenlesbarer Code

```
'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'
[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)
```

- QR
  - Standard JIS X 0510:2004

```
QR(MaschinenlesbarerCode)
```

- OCR
  - OCR-A Font

```
MaschinenlesbarerCode32
Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)
OCR-Druck(MaschinenlesbarerCode32)
```

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

```
lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))
```

  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:
Festlegungen des BMF

- Maschinenlesbarer Code

```
'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'
[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)
```

- QR
  - Standard JIS X 0510:2004

```
QR(Maschinenlesbarer Code)
```

- OCR
  - OCR-A Font

```
MaschinenlesbarerCode32
Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)
OCR-Druck(MaschinenlesbarerCode32)
```

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

```
lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))
```

  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:

Festlegungen des BMF

- Maschinenlesbarer Code

  `'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'`
  `[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)`

- QR
  - Standard JIS X 0510:2004

    `QR(Maschinenlesbarer Code)`

- OCR
  - OCR-A Font

    `MaschinenlesbarerCode32`
    `Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)`
    `OCR-Druck(MaschinenlesbarerCode32)`

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

    `lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))`

  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:

Festlegungen des BMF

- Maschinenlesbarer Code

  `'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'`
  `[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)`

- QR
  - Standard JIS X 0510:2004

    `QR(Maschinenlesbarer Code)`

- OCR
  - OCR-A Font

    `MaschinenlesbarerCode32`
    `Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)`
    `OCR-Druck(MaschinenlesbarerCode32)`

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

    `lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))`

  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:

Festlegungen des BMF

- Maschinenlesbarer Code

  `'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'`
  `[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)`

- QR
  - Standard JIS X 0510:2004

    `QR(Maschinenlesbarer Code)`

- OCR
  - OCR-A Font

    `MaschinenlesbarerCode32`
    `Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)`
    `OCR-Druck(MaschinenlesbarerCode32)`

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

    `lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))`

  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:

Festlegungen des BMF

- Maschinenlesbarer Code

  `'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'`
  `[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)`

- QR
  - Standard JIS X 0510:2004

    `QR(Maschinenlesbarer Code)`

- OCR
  - OCR-A Font

    `MaschinenlesbarerCode32`
    `Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)`
    `OCR-Druck(MaschinenlesbarerCode32)`

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

    `lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))`

  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:
Festlegungen des BMF

- Maschinenlesbarer Code

  `'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'`
  `[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)`
- QR
  - Standard JIS X 0510:2004

    `QR(Maschinenlesbarer Code)`
- OCR
  - OCR-A Font

    `MaschinenlesbarerCode32`
    `Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)`
    `OCR-Druck(MaschinenlesbarerCode32)`
- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

    `lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))`
  - GET -> json {"code"="maschinenlesbarerCode"}

QR/OCR/Link

Auf jeden Beleg anzudrucken: QR oder OCR oder Link, Details:

Festlegungen des BMF

- Maschinenlesbarer Code

  `'_R1-AT1_DEMO-CASH-BOX426_776730_2015-10-14T18:20:23_0,00_0,00_0,00_0,00_0,00_[...]_[SIGN]'`
  `[SIGN] ... dritter Wert der JWS Struktur (Base64URL -> Base64)`

- QR
  - Standard JIS X 0510:2004

    `QR(Maschinenlesbarer Code)`

- OCR
  - OCR-A Font

    `MaschinenlesbarerCode32`
    `Base64 -> Base32 für (Umsatzzähler, Sig-voriger-Beleg und Signaturwert)`
    `OCR-Druck(MaschinenlesbarerCode32)`

- URL
  - öffentlicher Link auf maschinenlesbarerCode, URL enthält {lnk}

    `lnk = base64Url(8bytes(sha256(MaschinenlesbarerCode)))`

  - GET -> json {"code"="maschinenlesbarerCode"}

AES Schlüssel

- AES-Schlüssel
  - wird in der Kasse generiert und BMF mitgeteilt
  - dient zum Verschlüsseln des Summenzählers
  - sollte nur Kasse und BMF bekannt sein
  - Wikipedia

AES Schlüssel

- AES-Schlüssel
  - wird in der Kasse generiert und BMF mitgeteilt
  - dient zum Verschlüsseln des Summenzählers
  - sollte nur Kasse und BMF bekannt sein
  - Wikipedia

AES Schlüssel

- AES-Schlüssel
  - wird in der Kasse generiert und BMF mitgeteilt
  - dient zum Verschlüsseln des Summenzählers
  - sollte nur Kasse und BMF bekannt sein
  - Wikipedia

AES Schlüssel

- AES-Schlüssel
  - wird in der Kasse generiert und BMF mitgeteilt
  - dient zum Verschlüsseln des Summenzählers
  - sollte nur Kasse und BMF bekannt sein
  - Wikipedia

AES Schlüssel

- AES-Schlüssel
  - wird in der Kasse generiert und BMF mitgeteilt
  - dient zum Verschlüsseln des Summenzählers
  - sollte nur Kasse und BMF bekannt sein
  - Wikipedia

Danke

- Vielen Dank für die Aufmerksamkeit
- Folien und Codebeispiele:
  - http://www.a-trust.at/registrierkasse
  - labs.a-trust.at
- Fragen ...
- Pause
- Democode