sparkle & AquaticPrime

Andreas Monitzer
2010-09-09

sparkle

free software updates for all

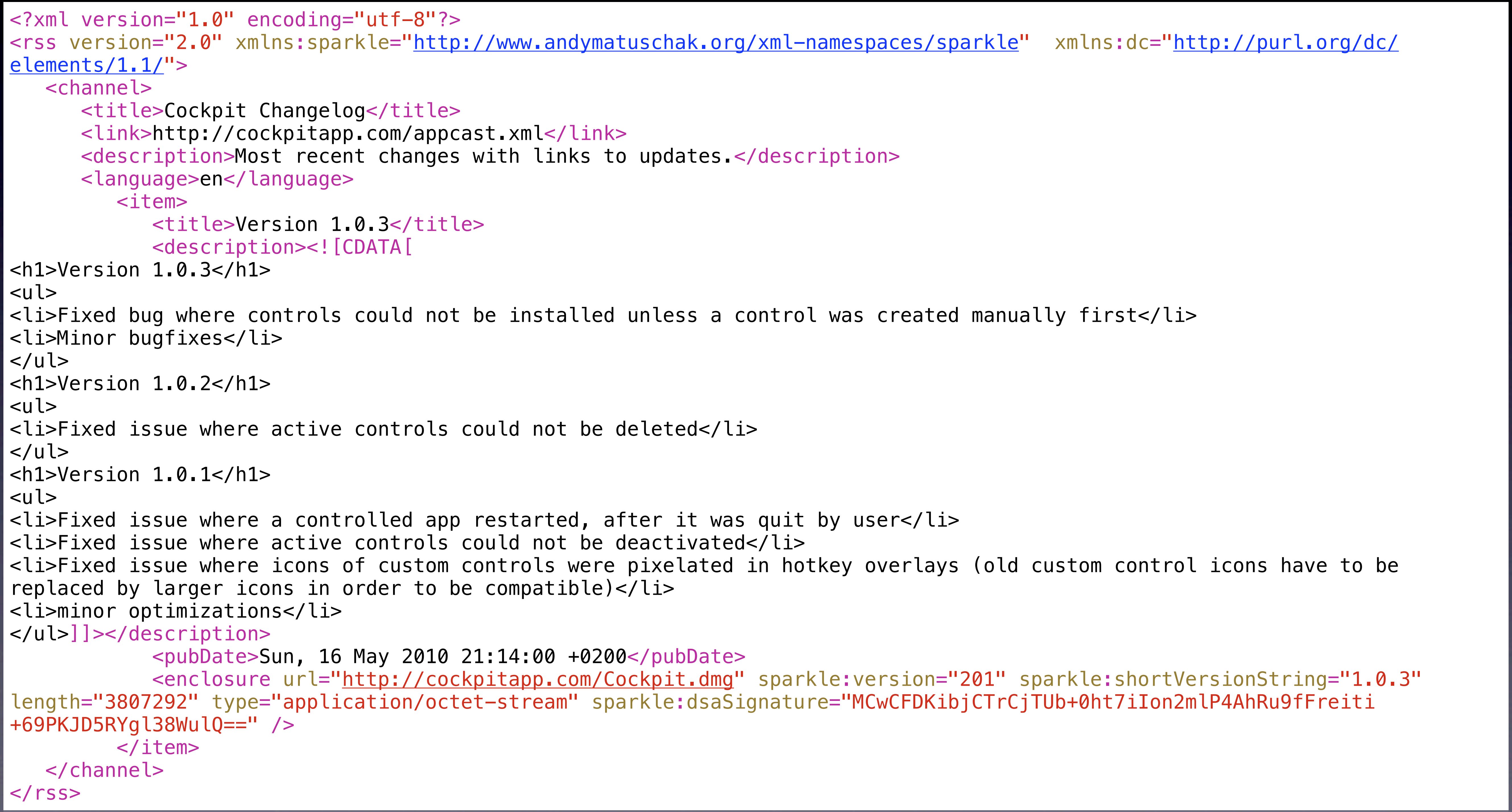
Features

- automatischer Updatecheck
- signierte Updates
- Open Source
- http://sparkle.andymatuschak.org/

Integration

- Sparkle.framework einbinden (mit link + copy build phase)
- SUUpdater instanzieren (in MainMenu.xib)
- DSA-Signatur erstellen & einbinden
- Info.plist anpassen

Serverseite



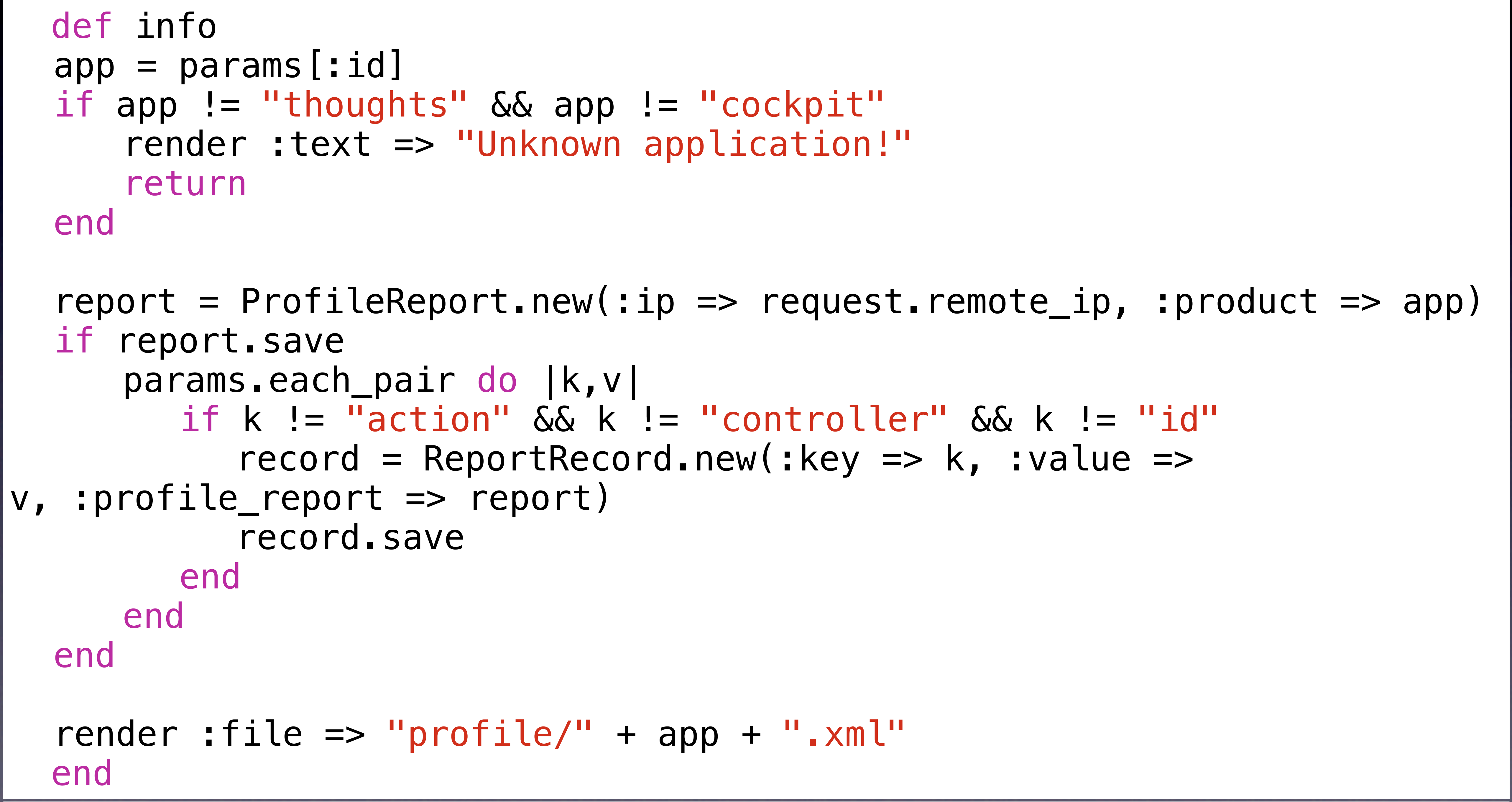
```
<?xml version="1.0" encoding="utf-8"?>
<rss version="2.0" xmlns:sparkle="http://www.andymatuschak.org/xml-namespaces/sparkle"  xmlns:dc="http://purl.org/dc/
elements/1.1/">
   <channel>
      <title>Cockpit Changelog</title>
      <link>http://cockpitapp.com/appcast.xml</link>
      <description>Most recent changes with links to updates.</description>
      <language>en</language>
         <item>
            <title>Version 1.0.3</title>
            <description><![CDATA[
<h1>Version 1.0.3</h1>
<ul>
<li>Fixed bug where controls could not be installed unless a control was created manually first</li>
<li>Minor bugfixes</li>
</ul>
<h1>Version 1.0.2</h1>
<ul>
<li>Fixed issue where active controls could not be deleted</li>
</ul>
<h1>Version 1.0.1</h1>
<ul>
<li>Fixed issue where a controlled app restarted, after it was quit by user</li>
<li>Fixed issue where active controls could not be deactivated</li>
<li>Fixed issue where icons of custom controls were pixelated in hotkey overlays (old custom control icons have to be
replaced by larger icons in order to be compatible)</li>
<li>minor optimizations</li>
</ul>]]></description>
            <pubDate>Sun, 16 May 2010 21:14:00 +0200</pubDate>
            <enclosure url="http://cockpitapp.com/Cockpit.dmg" sparkle:version="201" sparkle:shortVersionString="1.0.3"
length="3807292" type="application/octet-stream" sparkle:dsaSignature="MCwCFDKibjCTrCjTUb+0ht7iIon2mlP4AhRu9fFreiti
+69PKJD5RYgl38WulQ==" />
         </item>
   </channel>
</rss>
```

DEMO

Erweiterte Features

- System Profiling
- interne Build Numbers
- minimale Systemanforderungen definieren (Retter in der Not!)

System Profiling in RoR



```
 def info
  app = params[:id]
  if app != "thoughts" && app != "cockpit"
     render :text => "Unknown application!"
     return
  end

  report = ProfileReport.new(:ip => request.remote_ip, :product => app)
  if report.save
     params.each_pair do |k,v|
        if k != "action" && k != "controller" && k != "id"
           record = ReportRecord.new(:key => k, :value =>
v, :profile_report => report)
           record.save
        end
     end
  end

  render :file => "profile/" + app + ".xml"
 end
```

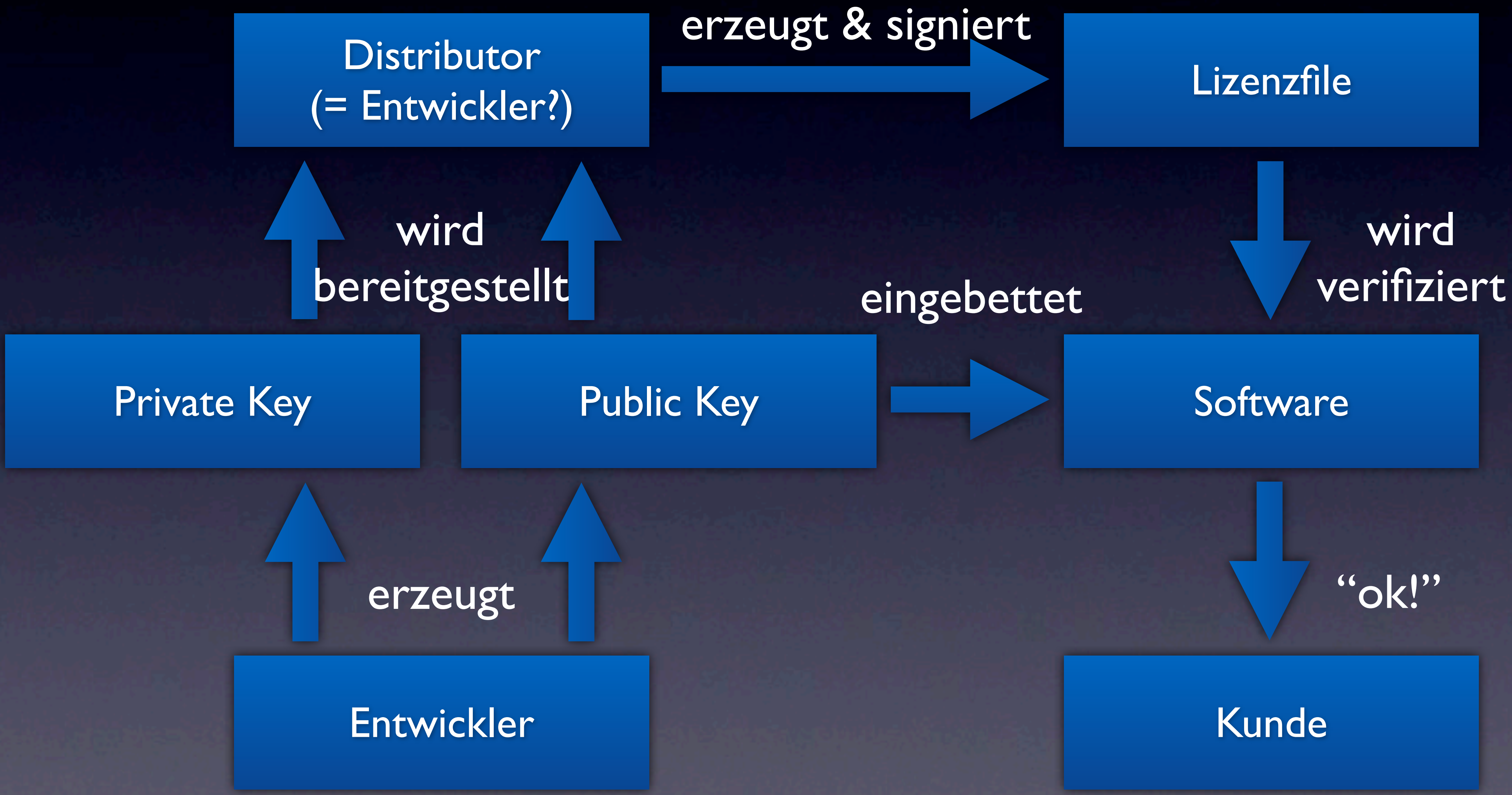
AquaticPrime

confidence with shareware.

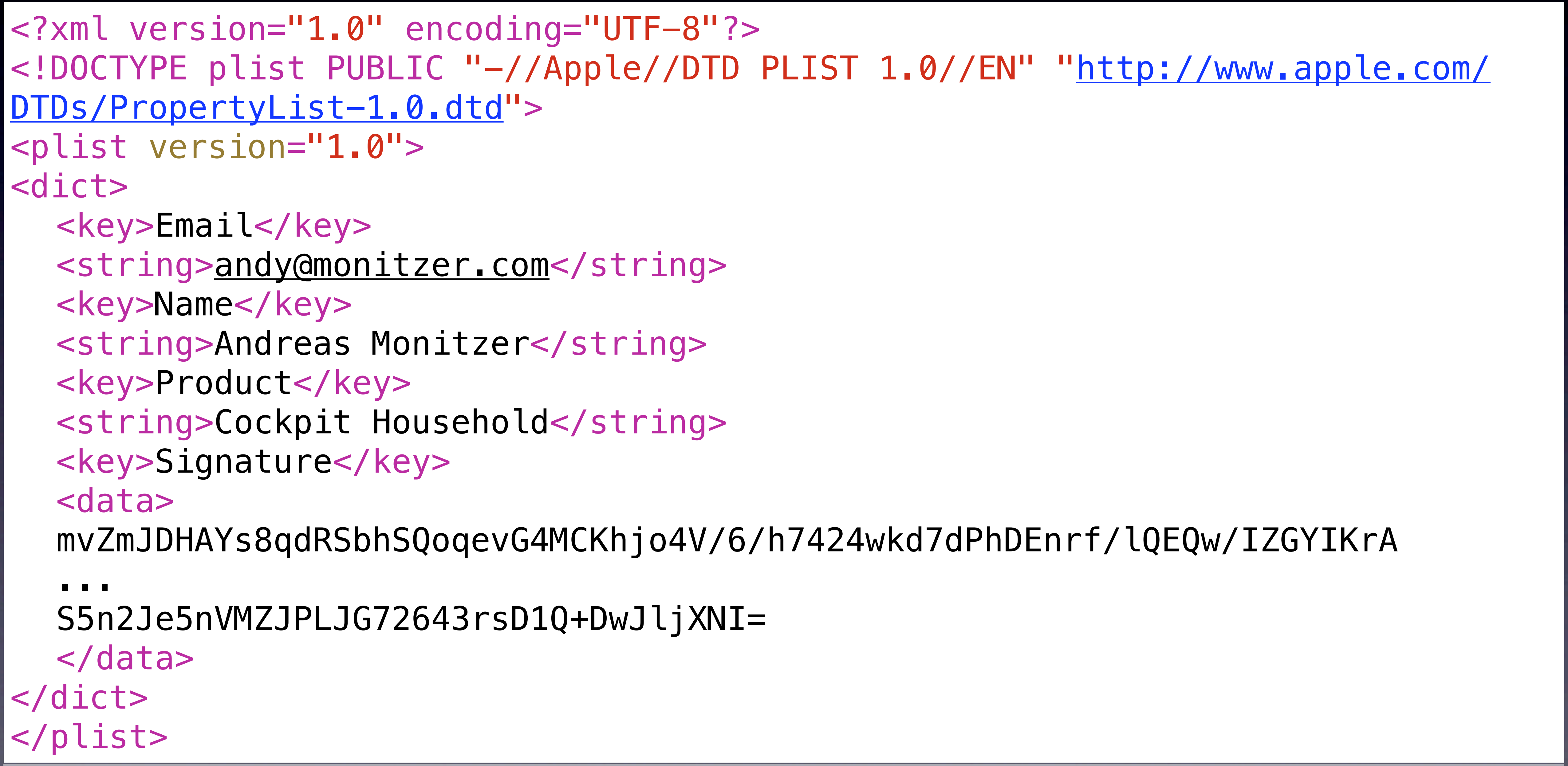
Features

- Generierung und Verifizierung von Softwarelizenzen
- asymmetrisches RSA
- http://www.aquaticmac.com/

Funktionsweise



Lizenzfile



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Email</key>
  <string>andy@monitzer.com</string>
  <key>Name</key>
  <string>Andreas Monitzer</string>
  <key>Product</key>
  <string>Cockpit Household</string>
  <key>Signature</key>
  <data>
  mvZmJDHAYs8qdRSbhSQoqevG4MCKhjo4V/6/h7424wkd7dPhDEnrf/lQEQw/IZGYIKrA
  ...
  S5n2Je5nVMZJPLJG72643rsD1Q+DwJljXNI=
  </data>
</dict>
</plist>
```

Vorgangsweise

- Lizenz anlegen in AP Developer
- libAquaticPrime.a und libcrypto.dylib einbinden
- Lizenzcheck einbauen
- Lizenzinstallation implementieren
    - application:openFile:
        - eigene Dateierweiterung!
    - Preferences anpassen

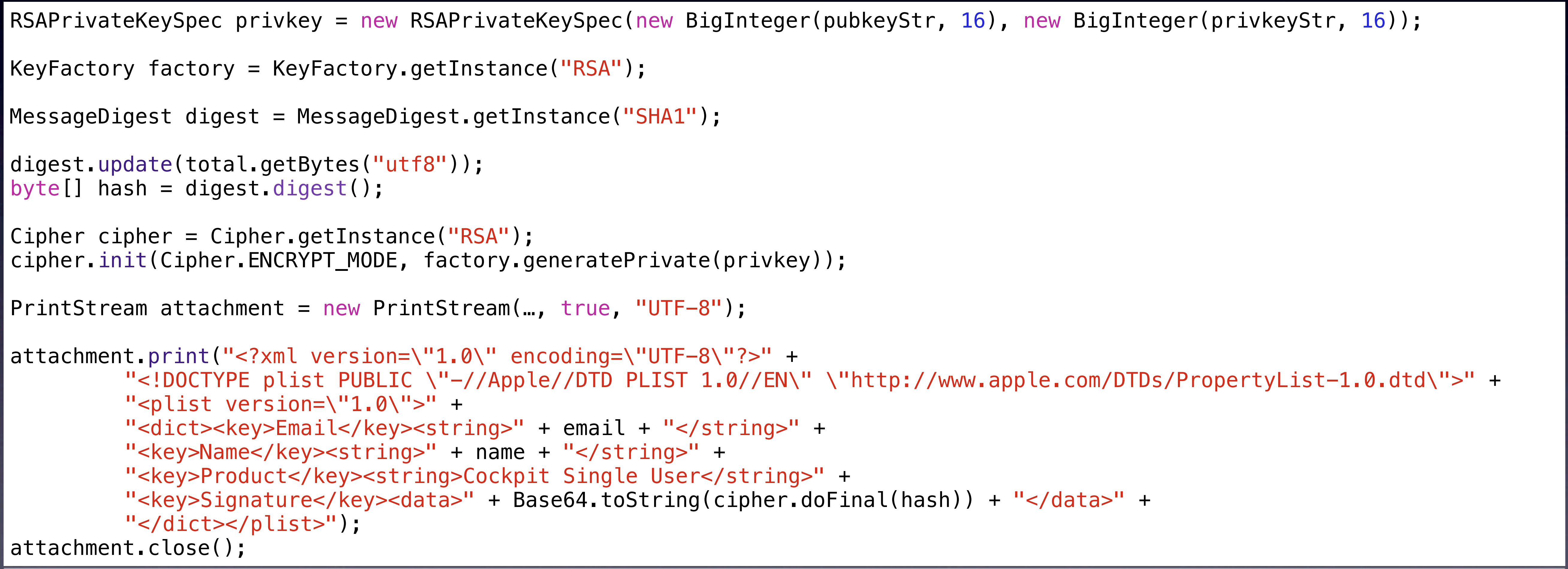
Vorteile

- fixfertige Lösung
  - Keygenerator-Applikation vorhanden
- kryptografisch einwandfrei, kein DRM
  - keine Keygeneratoren möglich
    (außer wenn private key entwendet wird)
- beliebige Zusatzinfos in Lizenzfiles

Nachteile

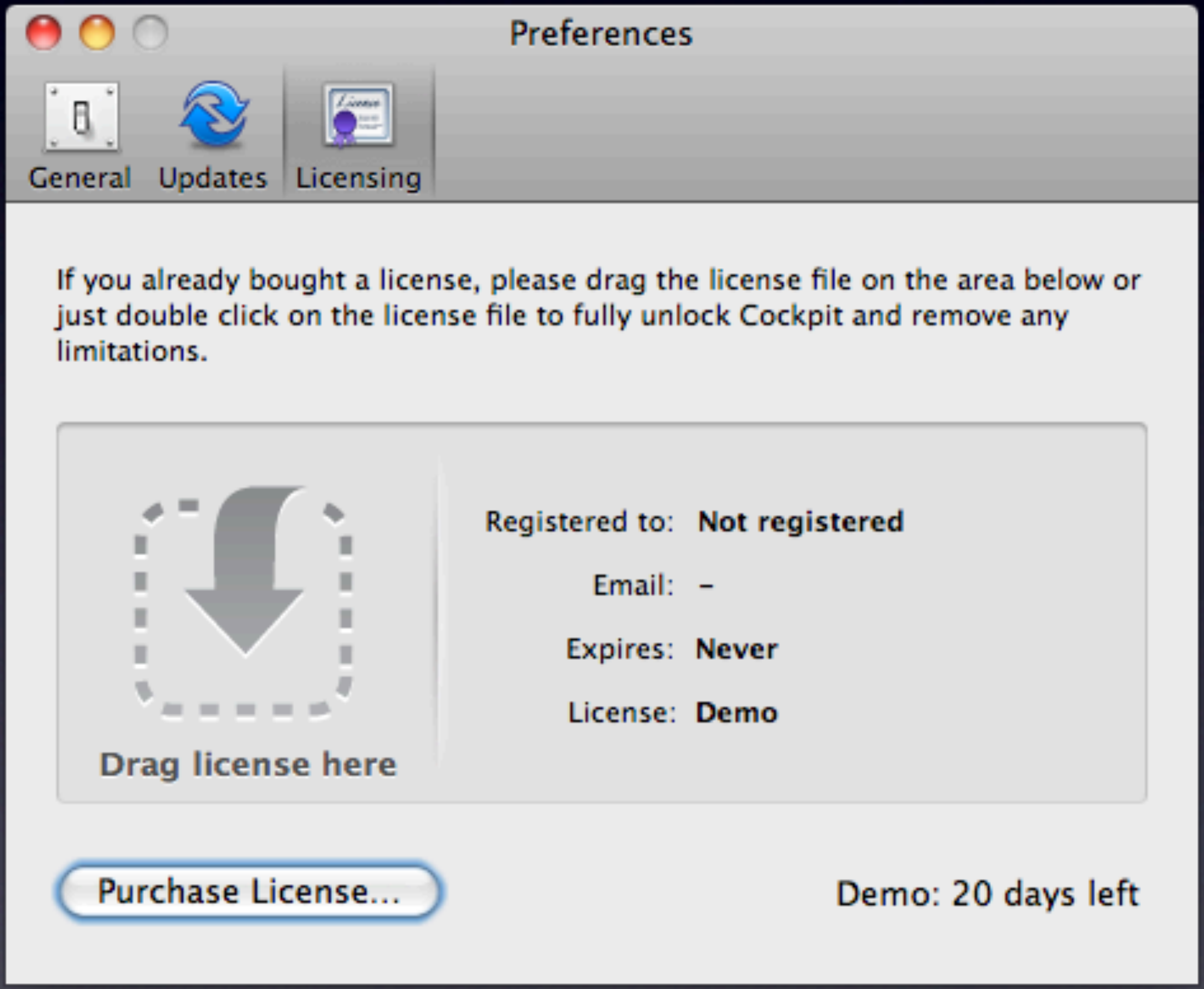
- leicht zu knacken da Open Source
  - einfach public key im Code mit eigenem ersetzen, oder AP-Klasse austauschen (APE)
- Lizenzfiles statt keys ein zweischneidiges Schwert
- keys nicht ganz trivial zu erzeugen
(zB. auf Google App Engine)
- Warum gibt es dazu nichts von Apple???

Google App Engine/Java



```java
RSAPrivateKeySpec privkey = new RSAPrivateKeySpec(new BigInteger(pubkeyStr, 16), new BigInteger(privkeyStr, 16));

KeyFactory factory = KeyFactory.getInstance("RSA");

MessageDigest digest = MessageDigest.getInstance("SHA1");

digest.update(total.getBytes("utf8"));
byte[] hash = digest.digest();

Cipher cipher = Cipher.getInstance("RSA");
cipher.init(Cipher.ENCRYPT_MODE, factory.generatePrivate(privkey));

PrintStream attachment = new PrintStream(…, true, "UTF-8");

attachment.print("<?xml version=\"1.0\" encoding=\"UTF-8\"?>" +
         "<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST 1.0//EN\" \"http://www.apple.com/DTDs/PropertyList-1.0.dtd\">" +
         "<plist version=\"1.0\">" +
         "<dict><key>Email</key><string>" + email + "</string>" +
         "<key>Name</key><string>" + name + "</string>" +
         "<key>Product</key><string>Cockpit Single User</string>" +
         "<key>Signature</key><data>" + Base64.toString(cipher.doFinal(hash)) + "</data>" +
         "</dict></plist>");
attachment.close();
```

User Interface



If you already bought a license, please drag the license file on the area below or just double click on the license file to fully unlock Cockpit and remove any limitations.

Drag license here

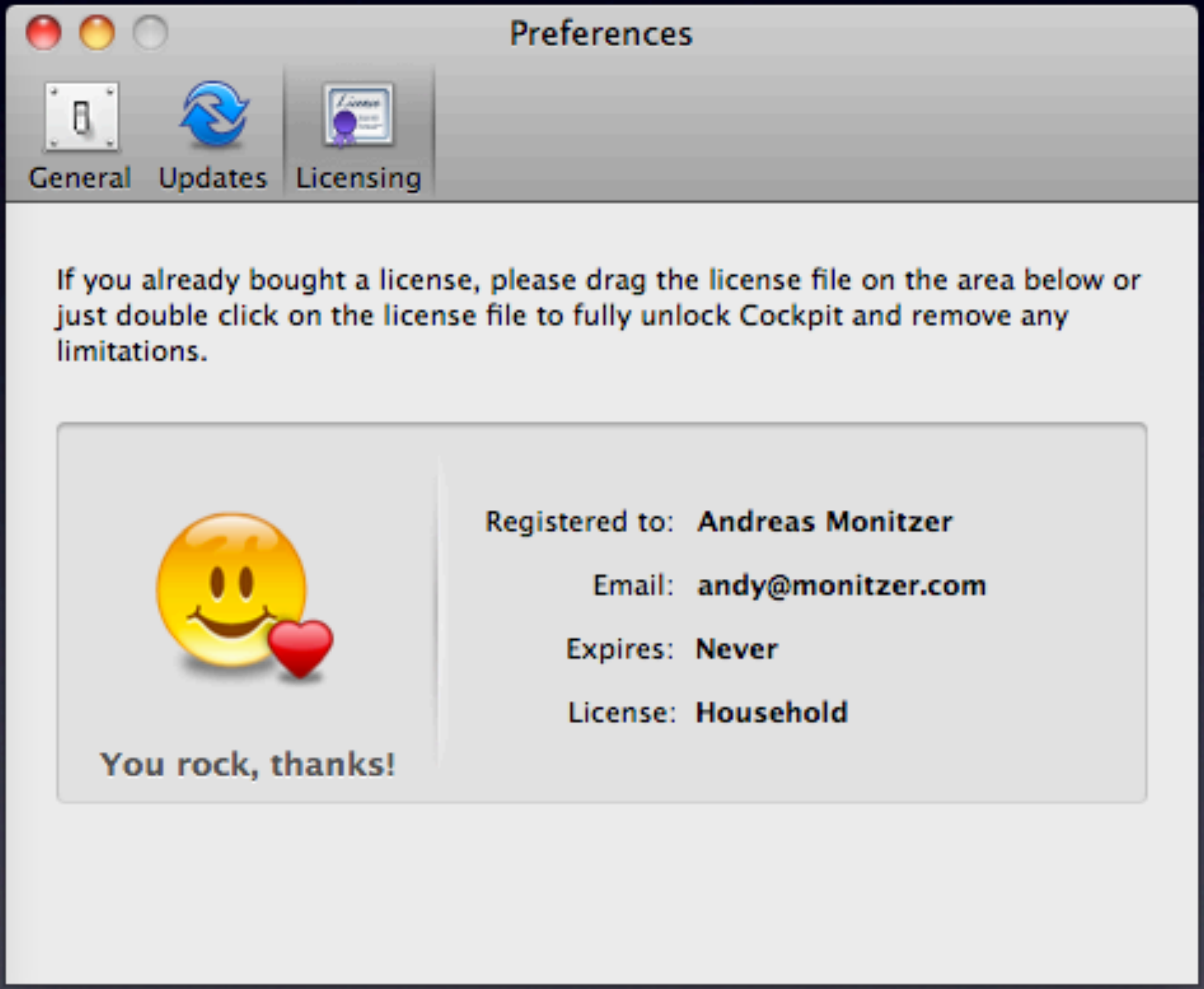
Registered to: **Not registered**

Email: **–**

Expires: **Never**

License: **Demo**

Demo: 20 days left



If you already bought a license, please drag the license file on the area below or just double click on the license file to fully unlock Cockpit and remove any limitations.

You rock, thanks!

Registered to: **Andreas Monitzer**

Email: **andy@monitzer.com**

Expires: **Never**

License: **Household**

DEMO