UCL Université catholique de Louvain

École polytechnique de Louvain (EPL)

Implementation Trade-offs for Access Tokens

Dissertation presented by
Nicolas COGNAUX

for obtaining the Master's degree in
Electrical Engineering

Supervisor(s)
François-Xavier STANDAERT , François KOEUNE , François MACÉ

Reader(s)
Edouard CUVELIER

Academic year 2015-2016

Acknowledgements

Confidential documents

This thesis concerns protected materials from NXP and STid. Confidential documents have been used for this work, those are listed in the bibliography and are subject to NDAs.

Technical explanations present in this thesis are related to public documents or open standards and nothing was published from those confidential documents. Those only served as reference for the implementation of the different upgrades (Transparent mode).

Licences

Libraries used in Chapter **??** such as GMP and libPBC are open-source and published under the LGPL which is given in appendix C.

Trademarks

- Android is a trademark of Google Inc.
- Blackberry is a trademark of BlackBerry Limited.
- Freescale is a trademark of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm.
- iPhone is a trademark of Apple Inc, registered in the US and other countries.
- MIFARE DESFire are registered trademarks of NXP B.V.
- NCS and Scaline are registered trademarks of NCS S.A.
- Qt is a registered trademark of The Qt Company Ltd.
- STid and Architect are registered trademarks of STid SA.
- Windows is a trademark of Microsoft Corporation in the United States and/or other countries.

Appendices

Appendix A

Material: Technical specifications

A.1 STid ARC-A

The ARC-A is the reader used in this thesis. It is compliant with NFC standard that allows it to communicate with smartphones. It embeds a PN532 (Manual is [**?**]) that allows to handle transparent mode of communication via SSCPV1 [**?**].

It uses the 13.56MHz frequency and is compliant with ISO 14443 types A and B [**?**]. More technical details can be found on the website of the manufacturer: `http://stid.com/catalog/index.php?id_product=342&controller=product&id_lang=1`.

A.2 Scaline SC415

The access controller used in this thesis is the SC415 from NCS Scaline. It embeds a Kinetis K61 as CPU. This CPU is ARM based (on 32 bits) and is clocked at 180 MHz. The Access controller includes 64 MB of RAM and 128 MB of Flash memory. The embedded Operating System (OS) is Linux based and include several useful libraries but not libGMP which was needed for the Proof Of Concept (see Chapter **??**).

More technical details can be found on the website of the manufacturer and in [**?**] and [**?**] from NCS Scaline.

Appendix B

Example of code using libPBC

This example, from library PBC_sig (`https://crypto.stanford.edu/pbc/sig/`) allows to understand the simplicity of libPBC. This example is the signature in the BB signature scheme which is pretty straightforward regarding the theory (see Chapter **??**).

```
void bb_sign(unsigned char *sig, unsigned int hashlen, unsigned char *hash,
    bb_public_key_t pk, bb_private_key_t sk)
{
  int len;
  element_t sigma;
  element_t r, z, m;
  bb_sys_param_ptr param = pk->param;
  pairing_ptr pairing = param->pairing;

  // Initialize element containers
  element_init(r, pairing->Zr);
  element_init(z, pairing->Zr);
  element_init(m, pairing->Zr);

  element_random(r);
  element_from_hash(m, hash, hashlen);

  // Perform the exponentiation of g_1
  element_mul(z, sk->y, r);
  element_add(z, z, sk->x);
  element_add(z, z, m);
  element_invert(z, z);
  element_init(sigma, pairing->G1);
  element_pow_zn(sigma, pk->g1, z);

  // Store the signature to byte array
  len = element_to_bytes_x_only(sig, sigma);
  element_to_bytes(&sig[len], r);

  // Clean memory
  element_clear(sigma);
  element_clear(r);
  element_clear(z);
  element_clear(m);
}
```

Appendix C

Lesser-GPL Licence

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

   As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

   "The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

   An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

   A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

   The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

   The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

   (a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

   (b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

   (a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

   (b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

   You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

   (a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

   (b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

   (c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

   (d) Do one of the following:

      . Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

      i. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

(e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

   You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

   (a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

   (b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

   The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

   If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

Rue Archimède, 1 bte L6.11.01, 1348 Louvain-la-Neuve **www.uclouvain.be/epl**