SRC
Security Research & Consulting GmbH

Emil-Nolde-Straße 7
D-53113 Bonn

Telefon: +49(0)228/2806-100
Telefax: +49(0)228/2806-199

E-mail: info@src-gmbh.de
Internet: www.src-gmbh.de

Rainer Landfermann
rainer.landfermann@src-gmbh.de
Durchwahl: -163

8. Juli 2016

Evaluierung des Utimaco CryptoServer CSe für den Einsatz in der Smart-Metering-PKI

Die SRC Security Research & Consulting GmbH ist beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Prüfstelle für die Evaluierung von Sicherheitskomponenten nach den Common Criteria (ISO 15408) anerkannt und erfüllt die Anforderungen der technischen Domänen „Smartcards and Similar Devices“ und „Hardware Devices with Security Boxes”.

Die vom BSI definierte „Certificate Policy der Smart Metering PKI“ (aktuell in Version 1.0.1) beschreibt die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von Zertifikaten in der Smart-Metering-Public-Key-Infrastruktur (SM-PKI). Dieses Dokument legt fest, dass die Teilnehmer der SM-PKI Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel verwenden müssen. Das Sicherheitsmodul CryptoServer CSe von Utimaco soll die Anforderungen erfüllen, die für den Einsatz bei den PKI-Teilnehmern Root-CA, Sub-CA, Externer Marktteilnehmer, Gateway-Administrator und Gateway-Hersteller[1] gestellt werden. Nach Kapitel 6.2 der Certificate Policy muss ein solches Sicherheitsmodul nach einem der Common-Criteria-Schutzprofile „Protection Profile Cryptographic Modules, Security Level ‚Standard‘“ (BSI-CC-PP-0079) oder „Protection Profile Cryptographic Modules, Security Level ‚Enhanced‘“ (BSI-CC-PP-0045) zertifiziert sein; jedoch kann diese Anforderung bis auf Widerruf alternativ durch folgende Nachweise erfüllt werden:

- Nachweis eines sicheren Zufallszahlengenerators aus einer der folgenden Klassen[2]: DRG.3 (bzw. DRG.4), PTG.3, NTG.1;
- Nachweis eines Tamper-Schutzes gegen Attack Potential „moderate“;
- Nachweis der Seitenkanalresistenz gegen Attack Potential „moderate“.

Diese Nachweise müssen durch eine durch das BSI für Common-Criteria-Evaluierungen anerkannte Prüfstelle erbracht werden.

---

[1] Definitionen der PKI-Teilnehmer siehe „Certificate Policy der Smart Metering PKI“, v1.0.1, Kapitel 1.3

[2] Definitionen der Klassen siehe Anwendungshinweise und Interpretationen zum Schema AIS 20/AIS 31, jeweils Version 3, 2013

Utimaco hat entschieden, die Anforderungen zunächst mittels der aufgeführten alternativen Nachweise zu erfüllen, und hat die Durchführung der entsprechenden Begutachtungen bei SRC beauftragt.

Die Begutachtungen wurden von SRC mit folgenden Ergebnissen abgeschlossen:

- Die Anforderungen an einen sicheren Zufallszahlengenerator der Klasse DRG.4 sind erfüllt.
- Die Schwachstellenanalyse des Tamper-Schutzes ergibt Resistenz gegen Attack Potential „high" (Resistenz des Tamper-Schutzes gegen das niedrigere Attack Potential „moderate" ist damit ebenfalls gegeben).
- Die Schwachstellenanalyse der Seitenkanalresistenz ergibt bei korrekter Nutzung der Kryptoalgorithmen Resistenz gegen Attack Potential „high" (Seitenkanalresistenz gegen das niedrigere Attack Potential „moderate" ist damit ebenfalls gegeben). Betrachtet wurden die folgenden Algorithmen:
    - AES-256
    - Diffie-Hellman Schlüsselaushandlung
    - ECDSA Signaturerzeugung und Signaturprüfung
    - ECDH Schlüsselaushandlung

Die Untersuchungen kommen somit zu dem Ergebnis, dass der Utimaco CryptoServer CSe die obengenannten Anforderungen der Certificate Policy erfüllt.

Detaillierte Ergebnisse der Begutachtungen wurden von SRC in Prüfberichten mit Stand von Juli 2016 dokumentiert.

Bei Fragen oder für weitere Informationen wenden Sie sich gerne an den Verfasser dieses Dokuments.

Mit freundlichen Grüßen

SRC Security Research & Consulting GmbH

Dr. Bertolt Krüger
Leiter der Prüfstelle

Rainer Landfermann
Abteilungsleiter