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

SRC
security consulting

Rainer Landfermann
rainer.landfermann@src-gmbh.de
ext. -163

08 July 2016

Evaluation of the Utimaco CryptoServer CSe for the German Smart Metering PKI

SRC Security Research & Consulting GmbH operates a Common Criteria (ISO 15408) security evaluation facility that is approved by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), and that fulfills the requirements for the technical domains "Smartcards and similar Devices" and "Hardware Devices with Security Boxes".

In its Certificate Policy of the smart metering public key infrastructure (PKI)[1], the BSI describes technical, personal and organisational security requirements for issuing certificates for the German smart metering PKI (SM-PKI). This document establishes that participants of the SM-PKI must use cryptographic modules for the generation, storage and use of their private keys. Utimaco's security module CryptoServer CSe is meant to fulfil the requirements set for the use by PKI participants "Root-CA", "Sub-CA", "Externer Marktteilnehmer" (external market participant), "Gateway-Administrator" and "Gateway-Hersteller" (gateway developer)[2]. According to chapter 6.2 of the Certificate Policy, this security module must be certified based on one of the Common Criteria Protection Profiles "Protection Profile Cryptographic Modules, Security Level 'Standard'" (BSI-CC-PP-0079) or "Protection Profile Cryptographic Modules, Security Level 'Enhanced'" (BSI-CC-PP-0045). Until cancelled, this requirement may alternatively be fulfilled by providing the following evidence:

- confirmation of a secure random number generator of one of the following classes[3]: DRG.3 (DRG.4, respectively), PTG.3, NTG.1;
- confirmation of tamper resistance against attack potential "moderate";
- confirmation of side channel resistance against attack potential "moderate".

This evidence must be provided by a Common Criteria evaluation facility that is approved by the BSI.

[1] "Certificate Policy der Smart Metering PKI", v1.0.1

[2] For definitions of the PKI participants see "Certificate Policy der Smart Metering PKI", v1.0.1, chapter 1.3

[3] For definitions of the classes see "Anwendungshinweise und Interpretationen zum Schema", AIS 20/AIS 31, BSI, each in version 3, 2013

Utimaco has decided to initially fulfil the requirements of the Certificate Policy by the listed alternative evidence, and has commissioned SRC to perform the corresponding evaluation.

SRC concluded the evaluation with the following results:

- The requirements for a secure random number generator of class DRG.4 are fulfilled.
- The vulnerability analysis of the tamper protection mechanisms showed that the HSM is resistant against attack potential "high" (which includes resistance against the lower attack potential "moderate").
- The vulnerability analysis of the side channel resistance showed that the HSM is resistant against attack potential "high" (which includes resistance against the lower attack potential "moderate") when the crypto algorithms are used correctly. The following algorithms were analysed:
    - AES-256
    - Diffie-Hellman key exchange
    - ECDSA signature generation and signature verification
    - ECDH key exchange

The evaluation therefore arrives at the conclusion that the Utimaco CryptoServer CSe fulfils the abovementioned requirements of the Certificate Policy.

Detailed results of the evaluation were documented by SRC in evaluation reports in July 2016.

In case of questions, please do not hesitate to contact the author of this document.

Kind regards

SRC Security Research & Consulting GmbH

Dr. Bertolt Krüger
Head of Evaluation Facility

Rainer Landfermann
Managing Consultant