UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
INSTITUTO TÉRCIO PACITTI
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

SÉRGIO DE MEDEIROS CÂMARA

UMA ARQUITETURA DE SEGURANÇA PARA MEDIDORES INTELIGENTES – verificação prática de dados de energia multitarifada

RIO DE JANEIRO
2012

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
INSTITUTO TÉRCIO PACITTI
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Sérgio de Medeiros Câmara

UMA ARQUITETURA DE SEGURANÇA PARA MEDIDORES INTELIGENTES - verificação prática de dados de energia multitarifada

Dissertação de Mestrado submetida ao Corpo Docente do Departamento de Ciência da Computação do Instituto de Matemática, e Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para obtenção do título de Mestre em Informática.

Orientadores: Luiz Fernando Rust da Costa Carmo, Dr.
Raphael Carlos Santos Machado, D.Sc.

RIO DE JANEIRO
2012

C172 Câmara, Sérgio de Medeiros
Uma arquitetura de segurança para medidores inteligentes – verificação prática de dados de energia multitarifada. / Sérgio de Medeiros Câmara. -- 2012.
95 f.: il.

Dissertação (Mestrado em Informática) Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti, Programa de Pós-Graduação em Informática, 2012.

Orientadores: Luiz Fernando Rust da Costa Carmo
Raphael Carlos Santos Machado

1. Arquitetura de Segurança. 2. Medidores Inteligentes. 3. Metrologia Legal – Teses. I. Carmo, Luiz Fernando Rust da Costa (Orient.). II. Machado, Raphael Carlos Santos. III. Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti, Programa de Pós-Graduação em Informática. IV. Título.

CDD

Sérgio de Medeiros Câmara

Uma arquitetura de segurança para medidores inteligente – verificação prática de dados de energia multitarifada

Dissertação de Mestrado submetida ao Corpo Docente do Programa de Pós-Graduação em Informática da Universidade Federal do Rio de Janeiro e à banca externa convidada como parte dos requisitos necessários para obtenção do título de Mestre em Informática.

Aprovada em: Rio de Janeiro 30 de Agosto de 2012.

Prof. Luiz Fernando R. C. Carmo – Orientador
Dr., UPS, França
PPGI/UFRJ

Prof. Raphael Machado – Orientador
D.Sc., COPPE/UFRJ, Brasil
INMETRO

Prof. Daniel Sadoc Menasche
Ph.D., UMASS, EUA
PPGI/UFRJ

Prof. Davidson Rodrigo Boccardo
D.Sc., UNESP, Brasil
INMETRO

Prof. Luís Henrique Maciel Kosmalski Costa
Dr., UPMC, França
COPPE/UFRJ

Rio de Janeiro
2012

Dedico à minha família e
à memória de Emília Ribeiro de Arruda Câmara e Hortêncio Catunda de Medeiros.

AGRADECIMENTOS

A Deus por me abençoar a cada dia, por abrir as portas permitindo que eu construa minhas oportunidades e por colocar cada uma dessas pessoas aqui lembradas pelo caminho da minha vida.

Aos meus amados pais, Ronaldo e Iracema, pelo exemplo de pessoas que são para mim, por toda educação e estrutura. Sem o amor e dedicação deles, este trabalho não seria possível.

À minha querida irmã, Viviane, minha amiga de todas as horas e de toda a vida, pelo seu carinho e apoio incondicionais. Aos demais familiares que, mesmo perto ou longe, sempre torceram por mim.

Ao professor e orientador, Luiz Fernando Rust, pelos ensinamentos, tempo e paciência, e pela confiança em mim depositada ao elaborar esta dissertação e ao integrar a sua equipe de trabalho.

Ao orientador, Raphael Machado, por todos os conhecimentos passados, as valiosas correções e revisões detalhadas de texto, e pelas nossas interessantes discussões sobre o tema.

Aos professores da banca examinadora, Davidson Boccardo, Daniel Sadoc e Luís Henrique Costa, por aceitarem o convite de participarem da minha defesa e pelas contribuições. Aos professores do PPGI/UFRJ, que estiveram presentes na minha formação e nos acompanhamentos de dissertação, em especial aos professores Adriano Cruz, Luci Pirmez e Paulo Aguiar.

Aos amigos da Ditel/Inmetro, por toda ajuda quando precisei e por fazerem do ambiente de trabalho um lugar descontraído mas com seriedade.

Aos amigos do LabNet, em especial aos ingressos nos anos de 2009 e 2010, pelos momentos de apoio mútuo, de estudo e de diversão.

À minha namorada, Sayonara, por estar presente e acompanhando de perto tudo o que acontece na minha vida. Suas palavras de entusiasmo e incentivo me confortam.

Aos irmãos do CPII, aos grandes amigos da banda Day7 e aos amigos que fiz na Módulo Security, pelo companheirismo, por torcerem sempre e por entenderem várias faltas minhas.

Ao Inmetro – Instituto Nacional de Metrologia, Qualidade e Tecnologia – pelo incentivo à pesquisa e aos meus estudos.

À Fundação de Apoio da Universidade Federal do Rio Grande do Sul, minha contratante desde que ingressei no Inmetro em Julho/2011.

À Universidade Federal do Rio de Janeiro, pela honra de ser e continuar fazendo parte desta instituição.

A todos, meus sinceros agradecimentos.

“If it doesn’t challenge you, it doesn’t change you.”

– Fred DeVito

RESUMO

Câmara, Sérgio de Medeiros. **Uma arquitetura de segurança para medidores inteligentes** – verificação prática de dados de energia multitarifada. 2012. 95 f. Dissertação (Mestrado em Informática) – Instituto de Matemática, Instituto Tércio Pacitti, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2012.

As Redes Elétricas Inteligentes estão sendo desenvolvidas em diversas partes do mundo de acordo com as necessidades de cada país. Devido a este cenário, os medidores de energia elétrica tornaram-se equipamentos complexos com o passar dos anos, agregando novas funcionalidades realizadas por *software*. Para as autoridades de Metrologia Legal, o esforço envolvido na análise de conformidade e aprovação de novos modelos de medidores aumentou imensamente, enquanto o correto funcionamento destes equipamentos ainda é questionado pela sociedade. Com o objetivo de estabelecer confiança nas medições de energia feitas por um medidor inteligente, este trabalho propõe uma arquitetura de segurança baseada em um módulo criptográfico (a "raiz de confiança" localizada no módulo de medição) e um autenticador de consumo. Este autenticador é gerado usando o esquema de assinatura digital ECPVS, o qual permite recuperação de mensagem. Nossa abordagem permite configurações de diferentes modalidades de energia multitarifada e apresenta quatro técnicas de composição da mensagem contida no autenticador, três destas considerando compressão lógica de dados. Nossas preocupações incluem o tamanho total desta mensagem e os dados necessários para validação do consumo em cada faixa de preço.

Palavras-chave: Arquitetura de segurança. Medidores Inteligentes. Metrologia Legal.

ABSTRACT

Câmara, Sérgio de Medeiros. **Uma arquitetura de segurança para medidores inteligentes** – verificação prática de dados de energia multitarifada. 2012. 95 f. Dissertação (Mestrado em Informática) – Instituto de Matemática, Instituto Tércio Pacitti, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2012.

Smart Grids are being deployed worldwide according to the needs that vary over different countries. Energy meters have become functionally complex over time, adding new features performed by software. For the Legal Metrology authorities, the effort involved on new smart meters type approval and conformity assessment keeps growing, whereas many concerns about the correctness of their behavior are still raised by society. Aiming at establishing trust on energy measurements taken by a smart meter, this work proposes a security architecture based on a cryptography module (the “root of trust” located on the metering module) and a consumption authenticator. This authenticator is generated using ECPVS digital signature scheme giving message recovery. Our approach allows different Time-Of-Use scenarios and presents four composing techniques for the authenticator's embedded message, the last three of them considering logical data compression. Our concerns are the final size of this message and the necessary data for validating the Time-Of-Use rates consumption values.

Keywords: Security Architecture. Smart Meters. Legal Metrology.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACD – Autenticador de Consumo Distribuído por Hora

AMI – *Advanced Metering Infrastructure*

ANEEL – Agência Nacional de Energia Elétrica

CP – Concentrador Primário

CRC-4 – *Cyclic Redundancy Check 4*

CS – Concentrador Secundário

CSWG – *Cyber Security Working Group*

ECC – *Elliptic Curve Cryptography*

ECDSA – *Elliptic Curve Digital Signature Algorithm*

ECNR – *Elliptic Curve Nyberg Rueppel*

ECPVS – *Elliptic Curve Pintsov-Vanstone Signature*

IEC – *International Electrotechnical Commission*

iNCE – Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Inmetro – Instituto Nacional de Metrologia, Qualidade e Tecnologia

ISO – *International Organization for Standardization*

KDF – *Key Derivation Function*

kWh – Quilowatt-hora

LABNET – Laboratório de Redes e Multimídia

MD5 – *Message-Digest algorithm 5*

MID – *Measuring Instruments Directive*

NIST – *National Institute of Standards and Technology*

OEB – *Ontario Energy Board*

OIML – *Organisation Internationale de Métrologie Légale*

PLC – *Power Line Communication*

PVM – Processo de Verificação da Medição

RTC – *Real Time Clock*

SCADA – *Supervisory Control and Data Acquisition*

SDMEE – Sistema Distribuído de Medição de Energia Elétrica

SHA – *Secure Hash Algorithm*

SMC – Sistema de Medição Centralizado

TMM – *Trusted Metering Module* (Módulo de Medição Confiável)

TOU – *Time-Of-Use*

UFRJ – Universidade Federal do Rio de Janeiro

SUMÁRIO

1 Introdução

As redes elétricas constituem um dos feitos tecnológicos mais notáveis do século 20. Com o passar dos anos, essas redes tornaram-se velhas e desatualizadas e muitos acreditam que elas não estejam, de fato, preparadas ou capazes de atender as demandas do século 21. O conceito de uma rede "inteligente" apresenta mudanças bastante significativas em relação às antigas, ao mesmo passo que também cria muitas oportunidades de negócio e desafios técnicos (DOE 2009).

As Redes Elétricas Inteligentes, ou *Smart Grids*, existem há pelo menos 25 anos. Porém, apenas recentemente, devido a fatores como a crise de energia global iminente, mudanças climáticas e o preço crescente dos combustíveis entre outros, elas começaram a chamar atenção entre os governos e a indústria. Durante os últimos anos, algumas empresas começaram a experimentar meios de tornar suas redes mais inteligentes, e os benefícios em potencial estão apenas começando a ser realizados.

Nos Estados Unidos da América, a **Energy Independence and Security Act (EISA)**, de 2007, estabeleceu uma política nacional de modernização da rede, criou comitês federais, definindo seus papéis e responsabilidades, e proporcionou incentivos aos investimentos de partes interessadas. Entretanto, antes da aprovação da lei **American Recovery and Reinvestment Act (ARRA)**, de Fevereiro de 2009, a indústria não estava certa se as Redes Inteligente*s* eram o futuro definitivo, já que não estava claro quem iria cobrir o investimento necessário para modernizar toda a rede. A injeção de U$11 bilhões na indústria americana para o desenvolvimento de Redes Inteligentes (THE WHITE HOUSE 2009), assim como o foco nesse tópico em alguns dos discursos do presidente americano Barack Obama, adicionaram confiança, direção e apoio às indústrias.

Para o país norte americano, um dos maiores motivadores para o desenvolvimento das Redes Inteligentes é lidar com o envelhecimento de seus ativos da rede elétrica, melhoria da qualidade de serviço, assim como a busca por novos modelos de negócio. Já para os países europeus, podemos destacar uma maior confiabilidade no sistema elétrico e as questões climáticas, como o uso de energias renováveis e diminuição do uso de combustíveis fósseis. No Japão, questões como um melhor gerenciamento energético, em função da escassez de recursos naturais, fortalecem a necessidade de implantação de uma rede de distribuição integrada e otimizada (CGEE 2011).

No Brasil, os investimentos em Redes Inteligentes chegarão a U$36,6 bilhões até o ano de 2022 (NORTHEAST GROUP 2012). Para o país, esses investimentos ajudarão a reduzir o **furto de energia** – o maior motivador até então – além de aumentar a confiabilidade da infraestrutura elétrica, oferecer novos planos de tarifação para os consumidores e permitir o crescimento da economia.

Como podemos perceber, no mundo todo existem inúmeras partes interessadas e comprometidas com os avanços da indústria e com o conceito de Rede Inteligente, como os órgãos reguladores, distribuidoras de energia elétrica, consumidores, fornecedores, organizações de pesquisa e a academia. Em meio a isso, o apoio dos governos se faz altamente necessário em todos os níveis de desenvolvimento.

Entretanto, para cada nova tecnologia introduzida no mercado, novas normas, requisitos, processos e testes precisam ser criados ou recriados para garantir seu sucesso. Entre os fatores-chave que se destacam como custo, disponibilidade e qualidade da energia e impacto ambiental, a segurança em todo seu âmbito é, sem dúvida, uma característica essencial a todo o sistema da rede elétrica. Especificamente, a **segurança da informação** está relacionada à integridade, privacidade e autenticidade dos dados que irão trafegar por essa grande rede. A violação de informações pessoais de consumidores e a alteração de comandos de controle são exemplos de como a confiabilidade no sistema de energia pode estar comprometida. Portanto, uma vez que os protocolos de comunicação usados na rede antiga eram muitos especializados e, como a "segurança por obscuridade" não é um conceito confiável, há uma grande necessidade de elaborar e implantar protocolos de segurança padronizados e bem documentados em substituição aos antigos (CLEVELAND 2008). Esse processo torna público o funcionamento das operações, abrindo espaço para ataques mais orientados.

As operações em um sistema de energia representam desafios de segurança que são diferentes da maioria das outras indústrias. A maioria das medidas de segurança existentes foi desenvolvida para combater *hackers* na internet, porém o ambiente da internet é muito diferente do ambiente operacional do sistema de energia. Além disso, na indústria da segurança, até há poucos anos atrás, existia uma falta de entendimento dos requisitos e dos possíveis impactos das medidas de segurança nas operações do sistema de energia.

Em 2009, o *National Institute of Standards and Technology* (NIST) estabeleceu um grupo chamado *Cyber Security Coordination Task Group* (CSCTG) para cuidar das questões de segurança relacionadas às Redes Inteligentes. Atualmente esse grupo integra o *Smart Grid*

Interoperability Panel (SGIP) e chama-se *Cyber Security Working Group* (CSWG). O CSWG possui mais de 500 membros voluntários dos setores público e privado, universidades, órgãos reguladores e agências federais (SGIP-CSWG 2010b). A segurança das Redes Inteligentes foi abordada pelo grupo em um projeto com um conjunto abrangente de requisitos de segurança cibernética de alta prioridade e críticos em todos os planos de aplicações. Esses requisitos são discutidos no documento *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, de Janeiro de 2010 (NIST 2010).

Ainda como parte desse projeto, o CSWG publicou um relatório de três volumes chamado *Guidelines for Smart Grid Cyber Security* que descreve uma estratégia mais detalhada de segurança cibernética para as Redes Inteligentes. Essas publicações compõem um conjunto inicial de base para os indivíduos e organizações responsáveis por tratar da segurança nos sistemas das Redes Inteligentes, e também nos subsistemas que são parte integrante dos componentes de *hardware* e *software* (SGIP-CSWG 2010a).

Um componente de grande importância para as Redes Inteligentes está localizado no domínio dos clientes, e é chamado de **medidor inteligente (*smart meter*)**. O medidor inteligente introduz diversas novas funcionalidades, em comparação aos medidores antigos, entre elas o registro em intervalos de tempo do consumo de energia elétrica de uma instalação e a entrega desses dados à distribuidora de energia, para fins de faturamento. Além disso, o medidor inteligente permite a adequação aos cenários de multitarifação de energia e informação de preço em tempo real ao consumidor, monitoramento e resposta à demanda, registro de eventos relevantes e comunicação bidirecional entre o aparelho e a central. Esta última característica inclui a troca de mensagens de controle, como por exemplo, o comando de habilitar/desabilitar remotamente o provimento de energia.

A entrada desses novos modelos de medidores no mercado depende de uma avaliação minuciosa e aprovação de uma autoridade metrológica. No Brasil, a **aprovação de modelos** de medidores inteligentes é realizada pelo **Inmetro – Instituto Nacional de Metrologia, Qualidade e Tecnologia**. O Inmetro tem como uma de suas funções a avaliação da conformidade dos modelos de medidores junto aos requisitos metrológicos e de *software*, atualmente especificados nas seguintes portarias em vigor: a Portaria Inmetro nº 431 de 2007 e a Portaria Inmetro nº 371 de 2007, referentes aos requisitos metrológicos e a Portaria Inmetro nº 11 de 2009 (futuramente substituída pela Portaria Inmetro nº 366 de 2011, em aprovação), referente aos requisitos de *software*.

Uma vez que um número cada vez maior de novas funcionalidades programadas por *software* começa a integrar o medidor inteligente, a atividade de aprovação de modelos tende a ser cada vez mais trabalhosa e complexa, demandando mais tempo de execução e profissionais envolvidos. Para a aprovação do *software* embarcado no medidor, a abertura, armazenamento seguro e análise de todo o código-fonte do medidor, além da análise da documentação completa de todas as suas funcionalidades, são exemplos de tarefas atualmente necessárias durante esse processo.

A fim de contornar essa situação, o Inmetro lançou um novo documento, a Portaria Inmetro nº 366 de 2011, o qual faz menção ao uso de arquiteturas especiais como uma forma de evitar uma análise total do código-fonte embarcado no medidor inteligente. Baseada nessa premissa, o presente trabalho propõe uma **arquitetura de segurança** desenvolvida com base no direcionamento e requisitos de segurança para os medidores inteligentes segundo a Metrologia Legal.

Além disso, a abordagem proposta no presente trabalho disponibiliza uma maneira onde os consumidores/usuários consigam também verificar e validar o funcionamento esperado do medidor inteligente, eliminado uma possível desconfiança de estarem sendo cobrados por valores de energia acima do realmente consumidos. Ademais, a proposta considera um cenário de multitarifação de energia elétrica, explicado na seção 2.1.2.

Quanto às contribuições, busca-se: (**i**) propor uma arquitetura de segurança para prover confiabilidade às partes interessadas em relação às medições realizadas pelo medidor inteligente, (**ii**) estabelecer uma maneira mais ágil de verificar o comportamento do *software* de novos modelos de medidores inteligentes, (**iii**) descrever um mecanismo de segurança em conformidade com os requisitos de segurança de *software* de um medidor inteligente segundo a Metrologia Legal brasileira, (**iv**) esboçar um módulo criptográfico seguro que servirá como "raiz de confiança" para o mecanismo de segurança, (**v**) elaborar técnicas de composição de um autenticador usado para a validação dos dados de medição de energia multitarifada, (**vi**) definir procedimentos externos ao medidor que complementem as soluções de segurança.

1.1 Motivação

Apesar de oferecer uma nova quantidade de benefícios, as Redes Inteligentes, e em especial os medidores inteligentes, apresentam muitos problemas de segurança que precisam ser reconhecidos e tratados.

Em Varodayan (VARODAYAN 2010), é descrito um problema no qual a falta de confiança no faturamento realizado pela concessionária gerou um problema de falta de privacidade dos dados de medição nas instalações dos clientes. Em 2009, os clientes da *Pacific Gas and Electricity* (PG&E), Califórnia, levantaram reclamações nas quais apontavam os medidores inteligentes como a causa de cobranças excessivas de preço. Dessa forma, vários clientes começaram a realizar medições redundantes através de um aparelho próprio de medição de energia, via conexão sem-fio sem proteção, para se certificarem o quanto estavam consumindo de fato. Caso esses clientes tivessem confiança, e pudessem ter a prova, de que os dados emitidos pelos medidores são genuínos, esse tipo de situação poderia ter sido evitada.

Em nCircle (2012), uma pesquisa recente aponta que 61% dos profissionais de segurança energética confirmam a insuficiência de controles de segurança em medidores inteligentes para proteção contra ataques de injeção de dados falsos. Esses ataques exploram as configurações vulneráveis das redes, introduzindo erros arbitrários em variáveis de estado e comprometendo técnicas de detecção de erros de medição. Esses fatos destacam um problema potencial de integridade dos dados que trafegam nas Redes Inteligentes.

Existem, portanto, grandes preocupações, de maneira geral, em relação à geração, integridade, privacidade e disponibilidade das informações armazenadas e enviadas entre o medidor, o consumidor e a concessionária de energia elétrica. Essas informações estão diretamente relacionadas a uma série de processos como a leitura e validação das medições pela concessionária e pelo consumidor, geração de conta, ativação/desativação do serviço, redução de roubo de energia, gerenciamento de demanda e do consumo de energia e envio de mensagens de controles e mensagens com conteúdo sobre pré-pagamento de energia (AMISEC-TF 2010). Esses processos, por sua vez, dependem do *software* embarcado no medidor, e serão considerados de confiança caso seja comprovada a validação desse *software.*

Para todo modelo de medidor inteligente hoje no mercado, é mandatório que este modelo seja testado e aprovado com base nos requisitos, metrológicos e de *software*, ditados por uma **autoridade metrológica**. No Brasil, o Inmetro – Instituto Nacional de Metrologia, Qualidade e Tecnologia – tem estabelecido documentação, procedimentos formais e capacitação de profissionais com finalidade de aprovar modelos de medidores inteligentes. Entretanto, apesar de todo esforço até hoje, o processo de validação de dispositivos dotados de *software* embarcado, como os medidores de energia, ainda é **dispendioso**. Garantir que o

software irá comportar-se exatamente como previsto pode requerer um esforço tão grande quanto o próprio esforço de desenvolvimento do mesmo.

Assim sendo, o *software* embarcado em um medidor inteligente **não pode ser considerado, em princípio, totalmente confiável**, isto é, não há garantias que este irá se comportar corretamente ou que este é exatamente o *software* validado durante a aprovação de modelos. A autoridade metrológica parte do princípio que os medidores inteligentes poderiam ser modificados posteriormente pelos consumidores, pelos fabricantes ou pela distribuidora de energia, para que ajam de maneira maliciosa de acordo com seus interesses.

Um exemplo de ataque que o consumidor pode sofrer é descrito na sequência. Os medidores convencionais, sem multitarifação de energia, apenas medem cumulativamente o total de energia consumida, logo alguém poderia forçar, por exemplo, um comportamento malicioso que incremente o contador total de energia mais rápido do que o normal, para tirar vantagem desse falso consumo extra todo mês. No entanto, medidores com suporte a **multitarifação** (horo-sazonal) podem ser adulterados de forma mais sutil – por exemplo, o total de consumo de energia continuaria inalterado, porém uma (pequena) porcentagem da faixa de preço mais barata de energia poderia ser adicionada às faixas de preço de pico, dessa forma, gerando contas de luz mais caras.

Por outro lado, os maiores adversários das concessionárias de energia mundiais tem sido os próprios consumidores que, tradicionalmente, são os principais atores em relação ao furto de energia. Alguns ataques referem-se a sobrescrever a aplicação (*firmware*) do medidor, através de *hack kits* disponibilizados por organizações criminosas, ou ainda a obtenção da senha do medidor para realizar comandos administrativos, a fim de interferir nos valores de consumo (MCLAUGHLIN *et al.* 2009).

No presente trabalho, abordarmos a problemática de **confiabilidade no medidor** envolvendo consumidores, concessionária e autoridade metrológica, e mitigamos também as questões envolvendo tempo e complexidade de uma validação de *software* embarcado em medidores inteligentes, em busca de um sistema confiável.

1.2 Objetivos

Nesse trabalho são identificados requisitos de segurança necessários aos medidores inteligentes baseados em documentos oficiais brasileiros de Metrologia Legal. Com base nestes, objetiva-se, de maneira geral, a elaboração de uma arquitetura de segurança capaz de

prover **confiabilidade no comportamento, autenticidade e integridade dos dados do medidor inteligente** para todas as partes interessadas, sendo elas o consumidor, a concessionária de energia elétrica e a autoridade metrológica, em um cenário de energia multitarifada.

Para isso, a arquitetura de segurança oferece mecanismos e meios para o consumidor conferir valores de consumos cobrados em sua conta, ou mesmo os valores exibidos no visor do seu medidor. Da mesma forma, as concessionárias de energia elétrica poderão se beneficiar de maneira a aumentar sua confiabilidade nos medidores em operação, uma vez que elas terão meios de checar se seus medidores sofreram algum tipo de adulteração que comprometa a integridade de seus dados.

A autoridade metrológica, responsável pela aprovação de modelos de medidores inteligentes, **reduziria o esforço empregado durante o processo de aprovação** e, como consequência, mitigaria os riscos associados à abertura e armazenamento de código-fonte proprietário dos fabricantes de medidores.

Como objetivos específicos, espera-se também: (**i**) estabelecer um mecanismo de segurança funcional em diferentes modalidades de multitarifação de energia, (**ii**) elaborar e testar técnicas de composição de um autenticador de consumo para medidores inteligentes e (**iii**) definir procedimentos externos que poderão ser realizados a partir do mecanismo de segurança proposto.

Além disso, é esperada a viabilidade dessa solução, mantendo-a compatível com um baixo custo de implementação.

1.3 Estrutura da Dissertação

Esta dissertação está dividida em seis capítulos, sendo a introdução o primeiro capítulo, onde é descrita uma contextualização e um melhor detalhamento sobre o escopo do problema abordado, nossas motivações e objetivos e as contribuições esperadas do trabalho.

No capítulo 2 são apresentados os conceitos que servem como base de conhecimento para este trabalho. Descrições sobre Redes Inteligentes, medidores inteligentes e multitarifação de energia elétrica são vistas mais a fundo. Um histórico da evolução da Metrologia Legal no Brasil relacionada à parte de energia elétrica e a infraestrutura adotada atualmente na distribuição da energia são abordados. Por fim, as explicações sobre assuntos

mais técnicos, como criptografia de chave-pública, assinatura digital e compressão de dados, também são realizadas ainda nessa parte do trabalho.

O capítulo 3 apresenta um conjunto de trabalhos relacionados, assim como sua relação com o assunto desta dissertação. Esses trabalhos estão divididos em três grupos principais que tratam de assuntos como aprovação e conformidade de modelos de instrumentos de medição atuais, trabalhos que tratam sobre a segurança, de maneira geral, relacionada a medidores inteligentes e, por fim, trabalhos que abordam o uso de assinaturas digitais com restrições de tamanho.

No capítulo 4 são apresentados os detalhes da arquitetura de segurança proposta. O esboço de um novo componente de *hardware* – um módulo criptográfico – será descrito, assim como suas funcionalidades, sua localização dentro de um medidor inteligente e os mecanismos de segurança envolvidos. O conceito de um autenticador de consumo será introduzido e, por último, descreveremos procedimentos externos ao medidor inteligente possíveis de serem realizados a partir desse autenticador, complementando a arquitetura de segurança como um todo.

O capítulo 5 apresenta diferentes técnicas de composição do autenticador de consumo. Essas técnicas são descritas, testadas e avaliadas a fim de se concluir qual técnica é mais apropriada aos requisitos do projeto. Além disso, outras duas abordagens para o autenticador de consumo também são apresentadas.

O capítulo 6 descreve uma análise de segurança acerca da arquitetura proposta, assim como um resumo de todo o trabalho e suas contribuições e sugestões para continuidade desta pesquisa.

2 Conceitos Básicos

Nesta seção são descritos os conceitos básicos que sustentam os temas abordados e são necessários para o entendimento do trabalho proposto.

2.1 Redes Elétricas Inteligentes

Na maioria dos países, os sistemas elétricos e de distribuição foram construídos quando a produção de energia era relativamente barata. O aspecto mais importante da confiabilidade da rede era baseado em ter capacidade em excesso, com um fluxo de energia unidirecional das usinas centralizadas para os consumidores. Os investimentos no sistema elétrico foram feitos a fim de atender a demanda crescente de energia e não para mudar fundamentalmente a maneira que o sistema funcionava. A falta de investimentos, aliado a vida útil de 40 anos ou mais dos ativos, resultou em um sistema elétrico **ineficiente e cada vez mais instável** (FEISST *et al.* 2008).

As mudanças climáticas, o preço cada vez mais alto dos combustíveis, a infraestrutura ultrapassada da rede e as novas tecnologias de geração de energia mudaram a mentalidade de todas as partes interessadas. As motivações chave que impulsionam a construção de uma rede inteligente são postas em quatro categorias: (**i**) melhorar a confiabilidade e segurança da rede, (**ii**) melhorar a eficiência operacional e os custos, (**iii**) equilibrar a oferta de geração e demanda de energia, e (**iv**) reduzir o impacto do sistema elétrico mundial nas alterações climáticas. As barreiras para essa transformação vão além de puras questões técnicas e econômicas, incluindo a falta de normas e de visão comum, modelos de regulação e negócios fragmentados e ultrapassados e a falta de consciência e confiança do público consumidor (PIKE RESEARCH 2009). O **gerenciamento da demanda** e o **monitoramento em tempo real** da rede se tornaram propostas promissoras para melhorar a eficiência energética, a confiança e utilização da rede, reduzir o consumo de energia como um todo e aumentar o retorno financeiro dos investimentos.

Em meio a tantas possibilidades, uma Rede Elétrica Inteligente deverá ser composta pelas seguintes características (ABB 2009a):

- **Adaptativa**, com menos dependência de operadores, em particular para responder rapidamente às mudanças de condições;

- **Preditiva**, em termos de aplicação de dados operacionais para manutenção de equipamentos e, até mesmo, identificar falhas potenciais antes que elas ocorram;
- **Integrada**, em termos de comunicação em tempo real e funções de controle (Figura 1);
- **Interativa** entre o mercado e os clientes;
- **Otimizada** para maximizar a confiabilidade, disponibilidade, eficiência e desempenho econômico;
- **Flexível**, para satisfazer as necessidades dos clientes, respondendo a novas mudanças;
- **Acessível**, concedendo acesso de conexão a todos os usuários da rede, especialmente para fontes de energia renováveis e com alta eficiência de geração local;
- **Confiável**, assegurando e melhorando a segurança e a qualidade da oferta, de acordo com as exigências dos tempos atuais, com capacidade de resistência a riscos e incertezas;
- **Econômica**, proporcionando o melhor valor através da inovação, gestão eficiente de energia, concorrência e regulação;
- **Segura** contra ataques e contra rupturas que ocorrem naturalmente.

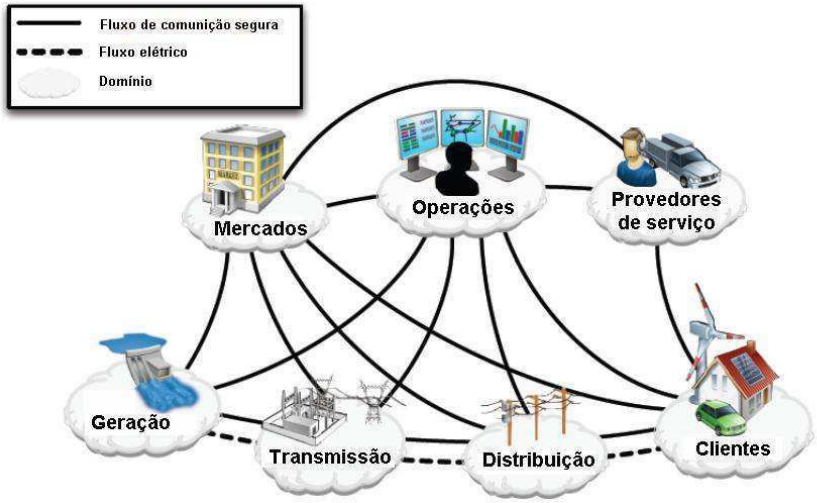

Figura 1. Modelo conceitual de rede inteligente (NIST 2010).

O desenvolvimento sistemático das redes de energia para incluir melhores controles, comunicações e uso de tecnologia moderna necessita a criação de dispositivos de automação

mais inteligentes e sistemas mais otimizados. Isso irá permitir que as distribuidoras de energia cumpram exigências de regulamentação e os consumidores usufruam de um fluxo de energia confiável de ambas origens de energia, convencional ou renovável (ABB 2009b). A criação de uma rede inteligente permite a **adição de todos os tipos de tecnologias da informação**, como medidores digitais, sensores e redes de comunicação para a internet ou para a comunicação legada. O desenvolvimento dessas tecnologias, aliado a sistemas de negócios, **abrem novas oportunidades em todos os níveis do sistema**, e permitem que os sinais do mercado impulsionem a eficiência técnica e comercial (HASHMI 2011).

No Brasil, a **ANEEL (Agência Nacional de Energia Elétrica)** tem atuado na regulamentação de tecnologias na área, conduzindo ações relacionadas ao tema, como: a discussão sobre padronização de medidores eletrônicos, a regulação na exploração de serviços de telecomunicações pelas empresas de eletricidade, a revisão completa da estrutura de tarifas, a definição de regulamentos para a conexão de microgeração às redes públicas de energia e o aprimoramento de regras para as revisões periódicas das tarifas das distribuidoras de energia.

A Política Energética Nacional brasileira atualmente tem, como foco principal, o **crescimento da oferta** ou **expansão dos sistemas**. Diferentemente do resto do mundo, a eficiência energética está em segunda prioridade, pois ainda há espaço para crescimento do consumo dos clientes. Como grande motivação, o Brasil mantém **o combate às perdas de energia**, que correspondem ao todo em torno de 17% da energia gerada. O furto, a fraude na medição e o desperdício de energia andam juntos, e os benefícios na recuperação dessas perdas podem efetivamente proporcionar tarifas mais baixas no curto prazo e amenizar a velocidade de construção de novas usinas e empreendimentos, consequentemente também reduzindo os impactos ambientais (BOCCUZZI 2012).

Em suma, os benefícios em potencial das redes inteligentes são muitos, mas o grande desafio é como eles serão alcançados. A implantação de tecnologias nas redes irá ocorrer ao decorrer de um longo período de tempo, adicionando sucessivas camadas de novas funcionalidades e capacidades em equipamentos e sistemas novos ou existentes. A tecnologia é uma questão fundamental para a construção e sucesso dessas novas redes.

2.1.1 AMI e Medidores Inteligentes

A AMI, *Advanced Metering Infrastructure*, **parte estrutural fundamental das Redes Inteligentes**, consiste do *hardware, software* e sistemas de comunicação e de gerenciamento de dados que possibilitam uma **rede bidirecional** entre os medidores de energia, os concentradores de dados (ou *gateways*) e os sistemas de negócios das concessionárias de energia. Dessa forma, os medidores inteligentes permitem a coleta e a distribuição de informação para os consumidores e outras partes, tais como os fornecedores de energia no varejo ou as próprias concessionárias (NIST 2010).

A AMI oferece aos consumidores os **preços de eletricidade em tempo real**, ou quase em tempo real, esquemas de **multitarifação de energia por postos tarifários** e pode ajudar as concessionárias na redução necessária de **carga de energia**. Isso permite que todas as partes tomem melhores decisões sobre reduções de custos e de tensão na rede durante os períodos de pico de demanda. A informação necessária sobre a demanda é acoplada junto à distribuição de energia. Essa informação é medida e agregada pelos chamados **medidores inteligentes,** os *smart meters*, que são medidores elétricos digitais que contém processador, armazenamento e interfaces de comunicação. Estes dois componentes, os medidores inteligentes e as redes de comunicação, formam a infraestrutura necessária para disponibilizar os serviços da AMI (MCLAUGHLIN *et al.* 2010).

Em termos gerais, os medidores inteligentes cumprem quatro funções básicas a respeito do gerenciamento de energia: (**i**) o monitoramento e gravação da demanda, (**ii**) registro em *log* de eventos relevantes de energia, como interrupções por exemplo, (**iii**) a entrega de informações de registro e uso de energia para a concessionária e (**iv**) a troca de mensagens de controle, permitindo, por exemplo, a desconexão remota do serviço. No entanto, o conceito de medição inteligente não está atrelado somente ao gerenciamento do consumo de energia de uma instalação, sendo assim, os medidores inteligentes também poderão ser usados para outras finalidades como medições de gás, água e condicionamento de ar.

Por sua vez, a infraestrutura de comunicação da AMI oferece uma interação contínua entre a concessionária, o consumidor e a carga elétrica controlável. Ela deve empregar padrões abertos de comunicação bidirecional, ser altamente segura e ter potencial para servir também como base para um grande número de novas funções da rede além da AMI. Várias arquiteturas podem ser implementadas, como uma das mais comuns, por exemplo, fazendo uso de **concentradores locais** que coletam dados de grupos de medidores e transmitem esses dados para um servidor central através de um *backhaul* (porção de rede responsável pela

ligação entre o núcleo da rede e as sub-redes periféricas). Vários meios podem ser considerados para fornecer parte ou a totalidade dessa arquitetura como: (**i**) *Power Line Communication* (PLC), (**ii**) *Broadband over power lines* (BPL), (**iii**) cabos de cobre ou de fibra óptica, (**iv**) comunicação sem fio (radio-frequência) centralizada ou distribuída, (**v**) Internet ou (**vi**) uma combinação de todas as anteriores (DOE 2008).

2.1.2 Estrutura Tarifária Horo-sazonal (Postos Tarifários)

A estrutura tarifária horo-sazonal, em inglês ***Time-Of-Use Tariffs*** **(TOU)**, é definida pela aplicação de tarifas diferenciadas de consumo de energia elétrica e de demanda de potência, de acordo com as **horas de utilização durante o dia e de acordo com o período do ano**. As tarifas horo-sazonais refletem o custo de produção de eletricidade em diferentes períodos. O preço da eletricidade, em geral, aumenta e diminui durante o curso do dia e tende a permanecer baixo durante a madrugada e nos finais-de-semana.

O objetivo dessa estrutura é **incentivar a racionalização da energia elétrica** durante os dias e durante o ano, esperando que haja uma mudança proativa no comportamento, por parte dos consumidores, para consumir mais energia elétrica durante os horários do dia que ela for mais barata, e evitar os períodos usualmente de maior demanda de energia (ANEEL 2005). Os períodos mais comuns se tratando de postos tarifários são: (**i**) fora-de-pico (*off-peak*), quando a demanda é baixa e as fontes mais baratas de energia são usadas, (**ii**) intermediário (*mid-peak*), quando o custo de energia e de demanda são moderados e (**iii**) pico (*on-peak*), quando há o máximo de demanda e onde as fontes mais caras de produção de energia são necessárias.

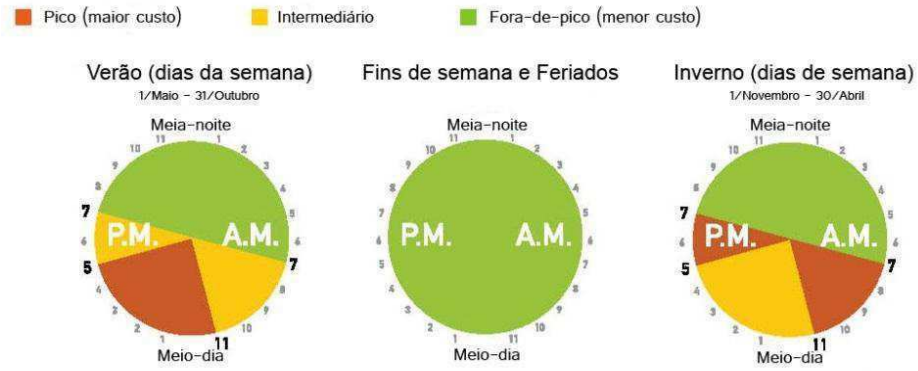

Figura 2. Configuração da modalidade tarifária do Ontario Energy Board (OEB 2012).

As tarifas por postos tarifários, ou TOU, são comuns em vários países desenvolvidos. A *Électricité de France* (EDF) opera o mais famoso exemplo de estrutura horo-sazonal. É estimado que um terço de seus 30 milhões de consumidores é adepto dessa estrutura tarifária,

a qual foi introduzida para consumidores residenciais voluntários em 1965, tendo sido primeiramente aplicada no país para consumidores de larga escala industrial em 1956. Nos EUA, a tarifas TOU são obrigatórias em vários estados, podendo a configuração variar de um estado para o outro. Como um exemplo, essas tarifas diferenciadas têm sido obrigatórias na Califórnia para todos os consumidores acima de 500kW desde 1978, como uma política estadual em resposta a uma crise de energia ocorrida em 1973 (COUSINS 2009).

No Canadá, o **Ontario Energy Board** (OEB) elaborou uma configuração de estrutura tarifária horo-sazonal onde são revisados os preços a cada seis meses. A configuração usada é a seguinte (Figura 2): durante os dias da semana do verão, o período de pico é de 11h às 17h e o período intermediário é de 7h às 11h e de 17h às 19h. Durante os dias da semana do inverno, o período de pico será de 7h às 11h e entre 17h e 19h e o período intermediário será de 11h às 17h. Para todas as estações, o período fora-de-pico é demarcado entre 19h e 7h, incluindo todos os fins-de-semana e feriados nacionais.

No Brasil, a ANEEL aprovou ao final de 2011 a **Tarifa Branca**, uma opção de modalidade tarifária para os consumidores residenciais de baixa tensão. A modalidade tarifária branca opcional abrangerá o subgrupo residencial com consumo médio mensal maior do que 200 kWh, de acordo com o plano de substituição de medidores a ser definido pela ANEEL. Consumidores residenciais com consumo maior do que 500 kWh serão enquadrados obrigatoriamente na Tarifa Branca, também seguindo esse plano de substituição de medidores (ANEEL 2010). A regulamentação inicial da nova modalidade estabeleceu um período de testes para 2013 e a previsão para entrada em vigor em 2014.

A modalidade inclui três postos tarifários, como segue: (**i**) Ponta, período de 3 horas consecutivas diárias com exceções aos sábados, domingos e feriados nacionais. O horário de Ponta é diferente para cada concessionária, dependendo de vários fatores ligados à região e mercado atendido, (**ii**) Intermediário, período formado pela hora imediatamente anterior e pela hora imediatamente posterior ao período de Ponta, totalizando duas horas por dia e (**iii**) Fora de Ponta, período composto pelas 19 horas complementares aos períodos de Ponta e Intermediário, bem como aos sábados, domingos e feriados. Um exemplo de configuração da Tarifa Branca é visto na Figura 3.

Figura 3. Exemplo de configuração da modalidade Tarifa Branca (ARGOZINO 2011).

A modalidade tarifária branca do Brasil e a modalidade tarifária da OEB do Canadá foram escolhidas para a parte de testes e simulações desta dissertação na seção 5.6.

2.2 Metrologia Legal e Redes Inteligentes no Brasil

Até a segunda metade dos anos 90, o Brasil adotava um modelo público de distribuição de energia elétrica. Esse modelo, por sua vez, era tolerante ao furto de energia, que naquela época totalizava aproximadamente **17% da energia total gerada no país**. Com a privatização das companhias de distribuição de energia, a ANEEL (Agência Nacional de Energia Elétrica) passou a responsabilizá-las por perdas não técnicas de energia, o que forçou a procura por soluções para esse problema e, por fim, a redução do furto de energia no território brasileiro (BOCCARDO *et al.* 2010).

No começo dos anos 2000, os medidores inteligentes começaram a ser instalados no Brasil, seguindo o padrão **SMC – Sistema de Medição Centralizado**. A arquitetura do SMC estipulava que os módulos de medições não mais estivessem localizados em cada residência e, sim, agrupados dentro de um concentrador, geralmente localizado no alto do poste de luz em meio às instalações de média tensão, para dificultar o acesso físico. Cada módulo de medição é associado a um dispositivo mostrador, o qual possui um visor onde são atualizados os valores de consumo de energia para cada unidade consumidora. Essa atualização é realizada através de uma comunicação sem-fio, como radiofrequência por exemplo.

Com o passar do tempo, após a implantação do sistema SMC, muitos medidores começaram a se comportar de maneira incorreta, em grande parte devido a **falhas de *software***. Devido a isso, houve uma necessidade de formalizar uma regulamentação sobre o SMC. Atualmente no Brasil, esses medidores inteligentes são aprovados de acordo com a Portaria Inmetro nº 371 de 2007 e a **Portaria Inmetro nº 11 de 2009**, a primeira metrológica e a segunda referente aos requisitos de *software*.

É de responsabilidade da **Autoridade Metrológica Legal**, no caso brasileiro o Inmetro (Instituto Nacional de Metrologia, Qualidade e Tecnologia), estabelecer quais elementos (*software, hardware* ou dados) do sistema de medição são legalmente relevantes. Para o Inmetro, são reconhecidos como **legalmente relevantes** todos os elementos, participantes da cadeia de medição, diretamente envolvidos ou que de alguma forma interfiram no processo de captura, processamento e publicação do resultado ao usuário final (INMETRO 2009). Segundo o Vocabulário Internacional de Termos Fundamentais e Gerais de Metrologia (Vocabulary of Metrology 2008), a **cadeia de medição** é uma "sequência de elementos de um instrumento ou sistema de medição que constitui o trajeto do sinal de medição desde o estímulo até a resposta".

O sistema SMC foi um primeiro estágio de medidores inteligentes adotados no Brasil para o que depois seria denominado **SDMEE (Sistema Distribuído de Medição de Energia Elétrica)**, uma opção de arquitetura mais amadurecida como solução de medições para a AMI.

2.2.1 Sistema Distribuído de Medição de Energia Elétrica

O SDMEE é capaz de assumir diferentes implementações de arquitetura. A seguir, é exposta uma implementação arquitetural do SDMEE que é, de forma geral, utilizada para a medição de energia elétrica em unidades consumidoras no Brasil (Figura 4). Essa implementação é composta basicamente por três equipamentos principais: (**i**) o Concentrador Primário (CP), (**ii**) o Concentrador Secundário (CS) e (**iii**) o Dispositivo Mostrador.

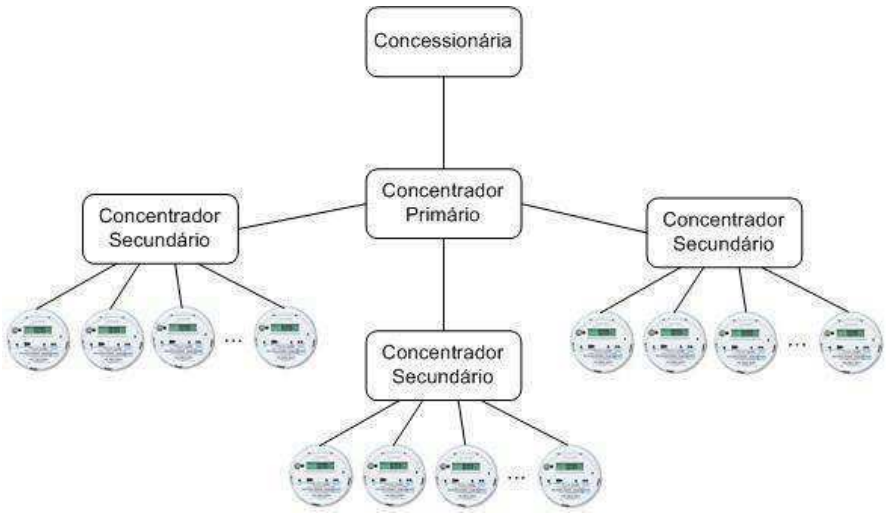

Figura 4. Diagrama da arquitetura SDMEE.

O **Concentrador Primário** é o equipamento responsável pela interface entre a concessionária de energia e os Concentradores Secundários. Ele realiza a aquisição periódica de dados provenientes dos CSs, monitoramento de alarmes desses equipamentos e sincronização de horário. Além disso, também permite o acesso remoto aos CSs para serviços de gerenciamento, leitura de dados e manutenção.

O **Concentrador Secundário** é o equipamento que abriga os módulos de medição responsáveis pelo cálculo do consumo de energia de cada residência. Nele também está contida toda a lógica de programação que contabiliza os dados gerados de cada módulo de medição e disponibiliza os dados de consumo ao consumidor. Sua segurança física, em geral, é confiada a uma caixa lacrada com sensores de abertura de porta. Além disso, é adotada a prática de fixar os CSs nos postes em meio à fiação de média tensão, com isso dificultando e **repelindo o acesso físico** ao equipamento, devido a um elevado risco de morte.

O **Dispositivo Mostrador** é a interface do sistema com o consumidor. Nele são mostrados basicamente os valores do consumo de energia, em kWh, e o horário no qual o visor foi atualizado. Em geral, a comunicação entre os dispositivos mostradores, CSs e o CP é feita através de radio frequência.

É importante ressaltar que não existe uma solução única de SDMEE para unidades consumidoras. Cada fabricante opta por funcionalidades, equipamentos, protocolos, metodologia e implementação mais apropriados para seu produto. Caberá à solução proposta o atendimento aos requisitos necessários, estipulados nas Portarias Inmetro, para que seja possível a sua aprovação e comercialização no território brasileiro.

2.2.2 Requisitos de software para Medidores Inteligentes

Diferentemente dos antigos medidores mecânicos de energia elétrica, os medidores eletrônicos e inteligentes compreendem **funcionalidades controladas por um *software* embarcado**. Esse *software* é responsável pela manipulação e tratamento dos dados medidos pelo equipamento, assim como também é responsável pelo seu armazenamento e disponibilização desses dados ao cliente e à distribuidora de energia.

Segundo a Metrologia Legal, o *software* embarcado no medidor também pode ser considerado legalmente relevante (definição na seção 2.2), incluindo toda aplicação e biblioteca de programação responsável pelo cálculo da medição, interferindo direta ou indiretamente sobre ele, assim também como as funções auxiliares de exibição, segurança,

checagem, transmissão/armazenamento de dados e carga de *software*. Por sua vez, também são legalmente relevantes, os componentes da interface de *software* protetora e toda variável, arquivo temporário ou parâmetro que gere alterações em valores, dados ou funções. Ademais, também haverá partes de *software* que pertençam aos módulos de *hardware* que não são legalmente relevantes, logo, estes também não são considerados legalmente relevantes e deverão ser separados do *software* que tem essa propriedade.

No Brasil, a regulamentação atualmente exigida para a **aprovação do *software* de um modelo de medidor inteligente**, como o SDMEE, está esclarecida na Portaria Inmetro nº 11 de 2009. O aspecto mais controverso desse regulamento é o requisito da **abertura do código-fonte** do *software* legalmente relevante para o Inmetro, que foi uma decisão resultante de uma ampla discussão com diversos fabricantes, influenciada pela complexidade arquitetural do sistema. Uma metodologia de avaliação foi desenvolvida para o SDMEE que incluía três passos: avaliação da arquitetura, checagem de integridade e validação do *software* (CARMO *et al.* 2009).

Em relação à validação de *software*, esse regulamento prevê requisitos para os seguintes aspectos, em resumo (INMETRO 2009):

- ***Software* embarcado para sistemas de medição**: o *software* deverá ser identificado, ter documentação, proteção contra mudanças, intencionais ou não, e proteção de parâmetros;
- **Transmissão de dados**: os dados transmitidos deverão ser completos, íntegros e autenticados e deverão ter proteção contra manipulação indevida, atrasos e indisponibilidade de serviços;
- **Separação de *software***: o *software* que não é legalmente relevante deverá ser claramente separado daquele que é. As informações geradas pelo *software* não legalmente relevante só podem ser exibidas caso não sejam confundidas com informações legalmente relevantes. Uma interface protetora deverá ser usada para a troca de dados entre os *softwares* legalmente relevantes e não relevantes.
- **Carga de *software***: o *software* carregado deverá ter sua autenticidade, integridade e rastreabilidade verificáveis. Sua carga e instalação deverão ter permissão explícita da concessionária e deverão ser automáticas, sem comprometimento do ambiente.

- **Auto-diagnóstico de falhas**: O *software* deverá ser capaz de diagnosticar um estado de mau funcionamento.
- **Dispositivo mostrador**: O dispositivo mostrador deverá ser capaz de registrar a energia correspondente à máxima corrente na maior tensão nominal e fator de potência unitário. Ele deverá cumprir, dentro de um tempo máximo, a atualização das informações mostradas.
- **Comportamento dinâmico**: o *software* legalmente relevante deverá sempre ter a disponibilidade necessária para o seu bom funcionamento, caso haja um compartilhamento de recursos de processamento.

Parte desses requisitos foi derivada de documentos de instituições internacionais, como a Norma WELMEC 7.2: *Software Guide – Measuring Instruments Directive* 2004/22/EC (Maio/2008) e também o Documento Internacional da Organização Internacional de Metrologia Legal – OIML D31/2008: *General Requirements of Software Controlled Measuring Instruments*. Esses documentos são comentados no capítulo 3, de Trabalhos Relacionados.

A **Portaria Inmetro nº 366 de 2011**, que até o fechamento desta dissertação não estava em vigor e se encontra em situação pós consulta pública, determina que os dispositivos relativos aos procedimentos de aprovação de modelo do regulamento aprovado pela Portaria Inmetro nº 11 de 2009 passarão a vigorar somente para os fabricantes com processos instaurados no Inmetro até a data de sua vigência (INMETRO 2011).

Além dos requisitos técnicos de *software* necessários ao processo de aprovação de modelo e a fim de garantir que o *software* legalmente relevante embarcado proporcione medidas corretas e dentro dos erros máximos admissíveis, essa nova Portaria também prevê o **uso de arquiteturas especiais baseadas em assinatura digital**. Dessa forma, ela permite que o sistema de medição possa fazer uso do mecanismo de assinatura digital para assegurar a autenticidade e irrefutabilidade das informações de medição. Ela define que poderão ser assinados dois tipos de informações: as grandezas de saída, ou seja, o valor acumulado em kWh, ou as grandezas de entrada, juntamente com informações que permitam reconstituir o valor da grandeza de saída. Isso se caracteriza uma vantagem, tanto para os fabricantes de sistemas de medição quanto para o Inmetro, pois a utilização desse tipo de arquitetura poderá **dispensar a entrega de parte da documentação** exigida na atual aprovação de modelos, facilitando e agilizando este processo.

2.3 Criptografia

Ao longo dos tempos, a criptografia tem sido uma arte praticada através da criação de técnicas específicas para atender alguns dos requisitos de segurança da informação. A partir de meados dos anos 70, essa disciplina esteve em um período de transição, passando de arte a ciência. Atualmente, existem várias conferências científicas internacionais dedicadas exclusivamente à criptografia e, também, uma organização científica internacional, a *International Association for Cryptologic Research* (IACR), que visa o fomento de pesquisas nesta área.

A **criptografia** é o estudo de técnicas matemáticas associadas a aspectos de **segurança da informação**, tais como (MENEZES *et al.* 1996):

1. **Confidencialidade** – um serviço usado para manter o conteúdo da informação apenas para aqueles autorizados a tê-lo. Termos sinônimos usualmente usados são “sigilo” e “privacidade”. Existem várias abordagens a fim de garantir a confidencialidade de uma informação, estas podendo variar desde uma proteção física a algoritmos matemáticos.

2. **Integridade de dados** – é um serviço que aborda a alteração não autorizada de dados. Para garantir a integridade, é preciso ter a capacidade de detectar a manipulação dos dados por partes não autorizadas. A manipulação inclui ações como a inserção, exclusão e substituição de dados.

3. **Autenticação** – é um serviço relacionado à identificação. Essa função se aplica tanto à informação quanto às entidades. Duas partes, ao iniciar uma comunicação, primeiramente devem se identificar mutuamente. A informação enviada por um canal deve ser autenticada em relação à origem, data de origem, conteúdo de dados, hora de envio, etc. Por estas razões, este aspecto da criptografia é usualmente subdividido em duas classes principais: a **autenticação da entidade** e a **autenticação da origem de dados**.

4. **Não-repúdio** – é um serviço que previne que uma entidade negue compromissos anteriores ou ações. Quando disputas acontecem devido a uma entidade ter negado que tomou determinadas ações, é necessário que seja envolvida uma terceira parte confiável para resolver esse tipo de situação.

Um objetivo fundamental da criptografia é abordar adequadamente estas quatro áreas, tanto na teoria quanto na prática. A criptografia é motivada pela prevenção e detecção de fraudes e outras atividades maliciosas.

A seguir, veremos algumas ferramentas criptográficas (primitivas criptográficas) que nos auxiliaram no desenvolvimento da nossa proposta.

2.3.1 Funções de Dispersão

Uma **Função de Dispersão**, ou *Hash Function*, é uma função computacionalmente eficiente que mapeia sequências binárias de tamanho arbitrário para sequências binárias de tamanho fixo, chamadas **valores de hash** (*hash-values*) (MENEZES *et al.* 1996).

Para uma função de dispersão que gera valores de hash de n bits (por exemplo, $n = 128$ ou 160), a probabilidade que uma sequência aleatoriamente escolhida seja mapeada para um valor de hash de n bits em particular é de 2^{-n}. A idéia básica é que um valor de hash sirva como uma representação compacta para uma sequência de entrada. Para ser de utilidade criptográfica, uma função de dispersão h é tipicamente escolhida de forma a ser computacionalmente inviável achar duas entradas distintas que geram o mesmo valor de hash (isto é, duas entradas x e y onde $h(x) = h(y)$), e que, dado um valor de hash específico y, seja computacionalmente inviável achar uma entrada x onde $h(x) = y$.

O uso mais comum de funções de dispersão em criptografia é para **assinaturas digitais** e para **integridade de dados**. Em relação a assinaturas digitais, uma mensagem longa é normalmente submetida a uma função de dispersão (usando uma função disponível publicamente) e apenas o valor de hash é assinado. A parte receptora da mensagem, por sua vez, submete também a mensagem à mesma função de dispersão, e verifica se a assinatura recebida está correta para este valor de hash. Isso poupa tempo e espaço de armazenamento se comparado à assinatura direta da mensagem. Note que a incapacidade de encontrar duas mensagens com o mesmo valor de hash é um requisito de segurança, pois, caso contrário, a assinatura de uma mensagem poderia ser a mesma de outra, permitindo que o signatário assine uma mensagem e, em um momento futuro, afirme ter assinado outra.

As funções de dispersão podem ser usadas para integridade de dados como segue. O valor de hash correspondente a uma entrada particular é computada em algum ponto no tempo. A integridade desse valor de hash é protegida de alguma maneira. Em um momento posterior, para verificar que os dados de entrada não foram alterados, o valor de hash é

computado novamente usando a entrada a ser verificada, e comparada com o valor de hash original. Algumas aplicações específicas incluem a distribuição de *software* e proteção contra vírus (MENEZES *et al.* 1996).

Duas funções de dispersão criptográficas populares são o MD5 e o SHA-1. O tamanho da saída da função MD5 é de 128 bits e da função SHA-1 é de 160 bits. O tamanho maior da saída do SHA-1 torna o "Ataque do Aniversário" (ataque que explora a probabilidade de encontrar colisões de valores de hash através de força-bruta) mais difícil, uma vez que, para o MD5, esse ataque necessita computar $\approx 2^{128/2} = 2^{64}$ valores de hash, enquanto que, para o SHA-1, tal ataque necessitaria computar $\approx 2^{160/2} = 2^{80}$ valores (KATZ e LINDELL 2007).

Diversos ataques a essas funções citadas, com a finalidade de encontrar colisões de valores de hash, foram realizados durante os anos 2000. Esses ataques motivaram uma mudança em busca de funções de dispersão mais fortes, com maiores tamanhos do valor de saída. Nesse sentido, destaca-se a família SHA-2, que estende a função SHA-1 e inclui funções de dispersão com saídas de tamanho de 224, 256, 384 e 512 bits.

2.3.2 Criptografia de Curvas Elípticas

A **Criptografia de Curvas Elípticas**, ou *Elliptic Curve Cryptography* (ECC), é uma **Criptografia de chave-pública**. Na Criptografia de chave-pública, cada usuário ou dispositivo participante de uma comunicação, em geral, possui um par de chaves, uma chave-pública e uma chave-privada, e um conjunto de operações criptográficas associadas a estas chaves. Apenas o usuário sabe sua chave-privada, enquanto sua chave-pública é distribuída para todos os usuários participantes da comunicação. A criptografia de chave-pública, diferentemente da criptografia de chave secreta, não exige que um segredo seja compartilhado entre os participantes, no entanto, apresenta um desempenho inferior à outra em relação ao tempo de processamento (MENEZES *et al.* 1996).

A segurança da criptografia de Curvas Elípticas depende da dificuldade do Problema do Logaritmo Discreto de uma curva elíptica, ou *Elliptic Curve Discrete Logarithm Problem* (*ECDLP*). Sejam P e Q dois pontos em uma curva elíptica tal que $kP = Q$, onde k é um escalar. Dados P e Q, torna-se computacionalmente inviável obter k, se k é suficientemente grande. O número k é chamado de logaritmo discreto de Q na base P.

Operações criptográficas requerem ser rápidas e precisas, no entanto, as operações sobre números reais são lentas e imprecisas devido a erros de arredondamento (RADHAMANI e

RAO 2007). Para que as operações em curvas elípticas sejam mais eficientes, a curva criptográfica pode ser definida sobre: (**i**) corpos finitos primos F_p ou (**ii**) corpos finitos de característica dois F_2^m.

A equação da curva elíptica sobre corpos finitos primos é definida por $\boldsymbol{y^2 \bmod p = x^3 + ax + b \bmod p}$, onde $\boldsymbol{4a^3 + 27b^2 \bmod p \neq 0}$. Os elementos do corpo finito são inteiros entre 0 (zero) e $p - 1$ e todas as operações, como adição, subtração, multiplicação e divisão, envolvem os inteiros nessa faixa. O número primo p é escolhido de forma que haja um número grande e finito de pontos na curva elíptica, possibilitando a segurança do sistema de criptografia.

A equação da curva elíptica sobre corpos finitos de característica dois é definida por $\boldsymbol{y^2 = x^3 + ax + b}$, onde $\boldsymbol{b \neq 0}$. Os elementos do corpo finito são inteiros de tamanho máximo de m bits. Estes números podem ser considerados como um polinômio binário, onde os coeficientes podem ser apenas ou 0 (zero) ou 1. Assim como p, o m também é escolhido de forma que haja um número grande e finito de pontos na curva elíptica, possibilitando a segurança do sistema criptográfico.

Cada valor de a e b resulta em diferentes curvas elípticas. Todos os pontos (x, y) que satisfazem a equação dada, mais um ponto no infinito, encontram-se na curva elíptica. A chave-pública é um ponto na curva e a chave-privada é um número aleatório. A chave-pública é obtida multiplicando a chave-privada por um ponto gerador G na curva. O ponto gerador G, os parâmetros da curva a e b, juntamente com algumas outras constantes constituem os **parâmetros de domínio** da criptografia de Curvas Elípticas. Esses parâmetros de domínio são um conjunto de constantes pré-definidas e conhecidas por todos os participantes de uma comunicação.

Uma vantagem principal da criptografia de Curvas Elípticas é o tamanho pequeno das chaves usadas. Uma chave ECC de 160 bits é considerada tão segura quanto uma chave RSA de 1024 bits. Além do armazenamento de chaves pequenas e devido também a sua complexidade computacional, a criptográfica de Curvas Elípticas é preferida para aplicações de redes sem-fio (LAUTER 2004).

2.3.3 Assinatura Digital

A assinatura digital é uma **primitiva criptográfica** fundamental em autenticação, autorização e não-repúdio. Seu propósito é oferecer meios para que uma entidade possa

vincular uma informação à sua identidade. O processo de assinatura implica em transformar a mensagem junto com uma informação secreta guardada pela entidade em uma marca, ou *tag*, chamada *assinatura*. Uma descrição genérica desse processo é mostrada na sequência. Primeiramente, definiremos algumas nomenclaturas (MENEZES *et al.* 1996):

- A é a entidade assinante e B é a entidade verificadora;
- M é o conjunto de mensagens que podem ser assinadas;
- S é o conjunto de elementos chamados *assinaturas*, isto é, todas as possíveis sequências binárias de um tamanho fixo;
- S_A é uma transformação do conjunto M para o conjunto S. A transformação S_A é mantida em segredo por A, e será usada para criar assinaturas de mensagens em M;
- V_A é uma transformação do conjunto $M \times S$ para o conjunto $\{verdadeiro, falso\}$. $M \times S$ consiste em todos os pares (m, s) onde $m \in M$ e $s \in S$. A transformação V_A é conhecida publicamente e é usada por outras entidades para verificar assinaturas criadas por A.

A entidade A cria uma assinatura para uma mensagem $m \in M$ da seguinte maneira:

1. Computar $s = S_A(m)$;
2. Transmitir o par (m, s), onde s é chamada de assinatura para a mensagem m.

Para verificar que uma assinatura s em uma mensagem m foi criada por A, uma entidade B deve realizar os seguintes passos:

1. Obter a função de verificação V_A de A;
2. Computar $u = V_A(m, s)$;
3. Aceitar a assinatura como criada por A se $u = verdadeiro$, e rejeitar a assinatura caso $u = falso$.

Um esquema de assinatura digital consiste de um **algoritmo de geração de assinatura** e um **algoritmo de verificação associado**. As transformações S_A e V_A oferecem um esquema de assinatura para A. De fato, essas transformações são tipicamente caracterizadas de forma mais compacta por uma **chave**, ou seja, existem classes de algoritmos de geração e verificação de assinatura publicamente conhecidos, e cada algoritmo é identificado por uma chave. Dessa forma, o algoritmo de geração de assinatura S_A é determinado por uma chave k_A

e A deve apenas manter k_A em segredo. De forma similar, o algoritmo de verificação V_A de A é determinado por uma chave l_A, esta sendo pública.

Existem **duas** classes gerais de esquemas de assinatura digital. Estas classes são descritas resumidamente a seguir:

1. Esquemas de **Assinatura Digital com Apêndice** – requerem a mensagem original como entrada para o algoritmo de verificação;
2. Esquemas de **Assinatura Digital com Recuperação de Mensagem** – não requerem a mensagem original como entrada para o algoritmo de verificação. Neste caso, a mensagem original é recuperada da própria assinatura (ver seção 2.3.4).

Em princípio, qualquer algoritmo de chave-pública pode ser usado para assinaturas digitais (TANENBAUM 2002). Dos algoritmos usados em esquemas de Assinatura Digital com Apêndice, destacam-se: (**i**) o **algoritmo RSASSA-PSS** (*RSA Probabilistic Signature Scheme with Appendix*), definida no padrão **PKCS#1**, primeiro da família de padrões chamada *Public-Key Cryptography Standards* (PKCS) publicada pela *RSA Laboratories*, com segurança baseada na fatoração de números inteiros, (**ii**) o **algoritmo DSA** (*Digital Signature Algorithm*), proposto pelo NIST em 1991, baseando sua segurança no problema do logaritmo discreto e (**iii**) o **algoritmo ECDSA** (*Elliptic Curve Digital Signature Algorithm*), baseado no algoritmo DSA e na abordagem da criptografia de Curvas Elípticas.

2.3.4 Assinatura Digital com Recuperação de Mensagem

Um esquema de Assinatura Digital com Recuperação de Mensagem é um mecanismo que **não requer o conhecimento da mensagem assinada** para execução do algoritmo de verificação. Na prática, apenas pequenas mensagens se aplicam a esse mecanismo, onde estas podem ser recuperadas de suas próprias assinaturas. Alguns exemplos de esquemas com recuperação de mensagem são o **RSA-PSSR** (*RSA Probabilistic Signature Scheme with Recovery*), o **NR** (Nyberg-Rueppel) e o **ECPVS** (*Elliptic Curve Pintsov-Vanstone Signature*) (MENEZES *et al.* 1996).

Alguns dos esquemas com recuperação de mensagem são especificados pelos seguintes padrões atualmente em vigor: (**i**) o **ISO/IEC 9796-2:2010 –** *Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms* e (ii) o **ISO/IEC 9796-**

3:2006 – *Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*. A ISO/IEC 9796-2:2010 especifica três esquemas de assinatura digital, dos quais dois são determinísticos e um é aleatório, e seus métodos de geração de chave correspondentes. A segurança destes três esquemas é baseada na dificuldade de fatoração de grandes números.

Por sua vez, a ISO/IEC 9796-3:2006 especifica esquemas de assinatura digital com recuperação de mensagem parcial ou total, com a finalidade de reduzir o *overhead* de armazenamento e transmissão. Ao todo, são seis esquemas que baseiam sua segurança no problema do logaritmo discreto de um corpo finito ou de curvas elípticas sobre corpos finitos. Além disso, a norma define tipos de redundância existentes em uma mensagem assinada: **redundância natural** e **redundância adicionada** (ISO/IEC 2006). Entre os esquemas citados, destacamos o ECNR (*Elliptic Curve Nyberg Rueppel*) que oferece recuperação total de mensagem e o ECPVS (*Elliptic Curve Pintsov-Vanstone Signature*) que oferece recuperação de mensagem parcial.

As assinaturas ECNR e ECPVS são ideais em sistemas de comunicação com largura de banda estreita onde toda, ou parte, da mensagem precisa ser mantida confidencial, conservando ainda características de uma assinatura segura e de tamanho pequeno (CERTICOM 2004). Como exemplo disso, a assinatura ECNR é a melhor opção para um sistema de RFID porque ela oferece troca de mensagens seguras com o menor gasto possível de energia (RULAND e LOHMANN 2007). O esquema ECNR forneceu a base para o desenvolvimento do esquema ECPVS. O ECPVS, por sua vez, melhora a eficiência sobre o ECNR oferecendo recuperação de mensagem parcial embutida na assinatura, ou seja, cabe ao assinante escolher qual parte da mensagem será embutida e qual será mantida em claro.

O esquema ECPVS é ideal para a criação de DPMs (*Digital Postal Marks*), uma tecnologia usada pelos serviços de correios para emissão de estampas confiáveis de tempo e de dados necessários que garantam a não-repudiação de um documento digital. Em se tratando de assinaturas de DPMs, o seu tamanho é importante devido ao fato da assinatura afetar o tamanho final da estampa. A assinatura ECPVS adiciona 20 bytes ao tamanho da mensagem original, o que significa ser **seis vezes menor** do que uma assinatura RSA e **metade** de uma assinatura ECDSA (CERTICOM 2004).

O processo de geração de uma assinatura ECPVS é descrito na sequência (ISO/IEC 2006). A entrada para o processo consiste dos parâmetros de domínio, a chave-privada x_A e uma mensagem M para ser assinada. Então, o assinante divide a mensagem M em $M_{clr} \,||\, M_{rec}$,

onde M_{clr} é a parte da mensagem enviada em claro e M_{rec} é a parte recuperável da mensagem. M_{clr} e M_{rec} devem ser formatadas e codificadas de maneira acordada anteriormente entre o assinante e o verificador. Seja d o dado de entrada M_{rec} (com redundância natural ou adicionada), n um número primo, k um inteiro aleatório no intervalo [1, n-1], π a chave simétrica computada por uma *Key Derivation Function* (KDF) a partir da chave-pública do assinante, a assinatura ECPVS deve ser computada pela seguinte, ou equivalente, sequência de passos:

1. Computar $r = Symmetric(d, \pi)$;
2. u = Hash(r || M_{clr});
3. Converta t = OS2IP(u); (octet-string-to-integer primitive function), note que t ϵ [0, n-1];
4. Se $t = 0$, então o processo de assinatura deve ser repetido com um novo valor aleatório k;
5. Computar $s = (k - x_A t) \ mod \ n$;
6. Se $s = 0$, então o processo de assinatura deve ser repetido com um novo valor aleatório k;
7. Apague k;

Gere como saída a assinatura (r, s) e a mensagem parcial M_{clr} (que pode ser nula).

O esquema de assinatura ECPVS é um dos candidatos a integrar um grupo de mecanismos a serem usados em sistemas embarcados, chamada Suite E - *Cryptographic Suite for Embedded Systems*, atualmente em elaboração no site do IETF - *Internet Engineering Task Force* (CAMPAGNA e ZAVERUCHA 2012).

2.4 Compressão de Dados

Compressão é o processo utilizado para reduzir o tamanho físico de um bloco de informação. A seguir, são descritas as principais características relacionadas à compressão de dados (MURRAY e VANRYPER 1996).

Os algoritmos de compressão de dados são usados para recodificar dados em uma representação diferente, mais compacta, com a finalidade de transmitir a mesma informação. A distinção entre os métodos de **compressão física** e **compressão lógica** é feita baseada em

como os dados são comprimidos ou, mais precisamente, como os dados são rearranjados de uma forma mais compactada.

A compressão física é realizada exclusivamente sobre os dados que a informação contém, apenas traduzindo uma série de bits de um padrão para outro mais compacto. Esses métodos de compressão tipicamente produzem sequências sem sentidos, mas que mantém uma relação com o conteúdo dos dados originais. Normalmente, o bloco resultante de dados comprimidos é menor que o original devido ao fato da eliminação da redundância existente nos dados originais. Por outro lado, a compressão lógica é realizada através de um processo de **substituição lógica**, ou seja, substituindo um símbolo numérico, binário ou do alfabeto por outro. Alterando o nome "Rio de Janeiro" para "RJ" é um bom exemplo de substituição lógica, pois "RJ" é derivado diretamente da informação contida em "Rio de Janeiro" e mantém algo sobre seu significado.

Os algoritmos de compressão podem ser divididos também entre duas categorias: **simétrico** e **assimétrico**. Um método de compressão simétrico utiliza basicamente os mesmos algoritmos para compressão e descompressão, realizando a mesma quantidade de trabalho para os dois. Os métodos assimétricos, por sua vez, requerem mais trabalho em uma direção do que na outra. Em geral, a etapa de compressão demanda mais tempo e mais recursos do sistema do que a etapa de descompressão, enquanto cenários para a situação inversa são menos comuns.

Alguns tipos de codificadores baseados em dicionário foram desenvolvidos para comprimir apenas tipos específicos de dados. Estes codificadores **não-adaptativos** contém um dicionário estático de sequências pré-definidas que são conhecidas por ocorrerem com alta frequência nos dados a serem codificados. Um codificador não-adaptativo desenvolvido especificamente para comprimir textos em inglês utilizaria um dicionário com sequência pré-definidas como "*and*", "*but*", "*of*" e "*the*", por aparecem frequentemente na língua inglesa. Por outro lado, um codificador **adaptativo** não apresenta heurísticas pré-concebidas sobre os dados a serem comprimidos. Estes compressores não possuem uma lista pré-definida de sequências estáticas e constroem seus dicionários a partir do zero, adicionando frases dinamicamente enquanto codificam. A compressão adaptativa é capaz de se ajustar a qualquer tipo de dados de entrada, enquanto a compressão não-adaptativa é capaz de codificar, de forma eficiente, apenas um seleto tipo de dados.

Por fim, existem métodos de **compressão de dados sem perdas** (*lossless data compression*) e métodos de **compressão de dados com perdas** (*lossy data compression*). Os

métodos são ditos com perdas quando os dados obtidos após o processo de descompressão não correspondem exatamente aos dados originais, de antes da compressão. No entanto, os dados descomprimidos mantem-se parecidos, de alguma forma, para que sejam úteis em algum propósito. Um exemplo de aplicação para a compressão de dados com perdas é a compactação de áudio e vídeo para divulgação na internet.

2.5 Conclusão

Este capítulo apresentou os conceitos básicos dos assuntos abordados nesta dissertação. Foram apresentados os conceitos gerais sobre Redes Elétricas Inteligentes, AMI (*Advanced Metering Infrastructure*) e medidores inteligentes, assim como a descrição das estruturas tarifárias horo-sazonais que estão sendo implantadas em diversas regiões do mundo e alguns exemplos de modalidades existentes.

Em seguida, relatamos os primeiros passos realizados no Brasil rumo à adoção das tecnologias de Redes Elétricas Inteligentes e o papel da Metrologia Legal durante esse processo. Descrevemos os novos modelos de medidores inteligentes, SMC e SDMEE, que foram desenvolvidos e os requisitos de *software* embarcado que esses modelos devem atender.

Introduzimos os conceitos de criptografia necessários para entendimento dos mecanismos usados neste trabalho, como funções de dispersão, criptografia de curvas elípticas, assinatura digital e assinatura digital com recuperação de mensagem. Por fim, descrevemos as principais características relacionadas à compressão de dados.

3 Trabalhos Relacionados

Neste capítulo são apresentados os trabalhos relacionados sob diferentes aspectos com a nossa proposta. Primeiramente, destacamos trabalhos que abordam requisitos de segurança para *software* embarcado em medidores e tratam da conformidade de novos modelos de medidores para aprovação pelas autoridades metrológicas. Em seguida, são apresentados trabalhos que propõe arquiteturas e soluções para assuntos gerais de segurança relacionados aos medidores, como confiabilidade, privacidade e autenticidade de dados. Por fim, são descritos alguns projetos que fazem uso de uma assinatura digital como mecanismo de segurança com restrições quanto ao seu tamanho total.

Uma vez que a segurança da informação desempenha um papel fundamental nas Redes Inteligentes, é necessário que o *software* embarcado nos medidores inteligentes atenda os requisitos de segurança estipulados pela autoridade metrológica de cada localidade e siga por uma avaliação estrita antes de sua aprovação. No Brasil, as portarias lançadas pelo Inmetro – Portaria Inmetro nº 11 de 2009 e Portaria Inmetro nº 366 de 2011 – citadas anteriormente neste trabalho, cumprem esse papel normativo. No âmbito internacional, podemos destacar dois documentos chave que serviriam de base para as portarias do Inmetro e que abordam os problemas envolvendo a avaliação de *software* embarcado, são eles: (**i**) o OIML D31/2009: *General Requirements of Software Controlled Measuring Instruments* e (**ii**) o WELMEC 7.2: *Software Guide – Measuring Instruments Directive* (2004/22/EC). Ambos os documentos estabelecem requisitos para *software* embarcado em instrumentos de medição.

O documento OIML D31/2009 disponibiliza um guia para a aprovação de modelos de instrumentos de medição e um conjunto de requisitos para verificação de conformidade do *software* embarcado nesses instrumentos de acordo com as recomendações da OIML – *Organisation Internationale de Métrologie Légale*. Os testes de conformidade abordam requisitos básicos (identificação do *software*, corretude dos algoritmos e funções), proteção do *software* (prevenção contra mal-uso e proteção contra fraudes), suporte para funcionalidades de *hardware* (durabilidade e detecção de falhas), separação de partes importantes e especificação de interfaces, portabilidade, manutenção e reconfiguração do *software*.

O documento WELMEC 7.2 oferece um guia para uma avaliação de conformidade de *software* de acordo com o *Measuring Instruments Directive* (MID), documento que estabelece os requisitos essenciais que os instrumentos de medição precisam satisfazer ao serem submetidos a um controle metrológico em algum estado-membro europeu. Esses requisitos

lidam com tópicos básicos (identificação de *software*, interfaces de comunicação e proteção contra mudanças acidentais ou intencionais), transmissão de dados, separação de *software*, *download* de *software* legalmente relevante, recuperação de falhas, comportamento dinâmico e adequação do dispositivo mostrador.

Na Alemanha, o processo de avaliação de medidores inteligentes é realizado baseado nas diretivas estabelecidas pelo WELMEC e pelo PTB – *Physikalisch-Technische Bundesanstalt* – o Instituto Metrológico Nacional alemão. Além dos medidores, a infraestrutura de distribuição alemã conta com um elemento a mais, um *gateway*, que concentra as funcionalidades relacionadas à segurança da informação, retirando estas dos medidores. Esse *gateway* tem mecanismos de *firewall*, comunicação segura, criptografia, autenticidade e integridade dos dados de medição, auditoria, atualização de *software*, tempo e dispositivo mostrador confiáveis (BSI 2011). Dessa forma, ao separar as particularidades dos medidores MID das funções de segurança da informação, o *gateway* pode ser submetido a uma avaliação de *Common Criteria*, de acordo com um *Protection Profile* apropriado. Além dessa vantagem, essa abordagem permite que os Organismos Notificados lidem de forma melhor com as dificuldades e limitações em envolver especialistas de segurança em TI em avaliações de medidores (INTEMANN 2011).

Alguns trabalhos que apresentam soluções e arquiteturas de segurança para assuntos relacionados aos medidores inteligentes são descritos a seguir. Em Molina-Markham *et al.* (MOLINA-MARKHAM *et al.* 2010), os autores demonstram que, através de métodos estatísticos e algoritmos de agrupamento (c*lustering*), é fácil extrair padrões de utilização da energia elétrica dos dados de um medidor inteligente. Logo, é possível determinar tipos específicos de atividades, sendo capaz de responder perguntas tais como quantas pessoas estão na casa em um dado momento, quais seus hábitos, etc. entre outras preocupações apresentadas em Quinn (QUINN 2009). Essas informações, aliadas a poderosas ferramentas analíticas, poderiam ser usadas em benefícios de companhias e/ou criminosos. Para tanto, o artigo propõe um esboço de uma arquitetura para medidores inteligentes que garante a privacidade dos consumidores, utilizando concentradores (*gateways*) confiáveis para armazenamento de dados anônimos de consumos de energia de um conjunto de medidores. Em relação ao valor da conta de luz, cada medidor calcula seu total e o envia à distribuidora de energia. Para que a distribuidora tenha confiança no valor reportado por determinado medidor, inicia-se entre eles um protocolo de Conhecimento Zero (*Zero-Knowledge*) onde, através de rodadas de perguntas e respostas, a distribuidora consegue inferir se tal valor é

verdadeiro. Dessa forma, a distribuidora não tem acesso aos dados de energia consumida por períodos de tempo das residências, o que garante a privacidade dos dados de utilização de energia pelos consumidores. Essa proposta se mostra complementar à nossa arquitetura, uma vez que ela oferece uma solução para a privacidade dos dados de consumo de energia considerando uma distribuidora confiável, enquanto que, por outro lado, o nosso projeto oferece soluções para verificação de integridade de dados de consumo considerando ambos, consumidores e distribuidora, não confiáveis.

Em Varodayan *et al.* (VARODAYAN *et al.* 2010), o foco do problema está em garantir para o consumidor a integridade dos dados de consumo de energia exibidos em sua conta de luz, sem comprometer sua privacidade. O cenário em questão prevê que os consumidores já estejam realizando um monitoramento pessoal do uso de energia, ocasionado pela falta de confiança nos dados de faturamento, através de um dispositivo sem-fio independente. O artigo explica que, através de uma análise feita nesta conexão sem-fio por um *eavesdropper*, é possível a detecção de atividades corriqueiras de uma residência, como o uso do chuveiro, televisão, etc. A solução proposta é a compressão dos dados redundantes de medição, que são mandados ao dispositivo verificador, a uma taxa abaixo de sua entropia (ou seja, com perdas) de tal forma que eles não possam ser revelados através dos bits codificados. Os dados no dispositivo verificador, no entanto, só poderão ser recuperados em conjunto com dados específicos reportados na conta de energia pela empresa distribuidora. Diferentemente, nossa proposta oferece uma solução para garantir a integridade dos dados de consumo gerados pelo medidor inteligente, além de elaborar um procedimento de verificação dos valores de consumo exibidos na conta de luz para o consumidor. Dessa forma, a prática de medição redundante através de um segundo dispositivo não seria necessária para o consumidor para validar o valor da conta recebida.

O artigo de Efthymiou *et al.* (EFTHYMIOU *et al.* 2010) tem também seu foco voltado à privacidade dos dados dos medidores inteligentes e propõe uma solução que garante o anonimato dos dados com alta frequência de medição, sem comprometer as operações da concessionária de energia e da rede de distribuição. A mudança propõe o uso de dois números identificadores embutidos no medidor inteligente em tempo de fabricação, o HFID (*High-Frequency* ID) e o LFID (*Low-Frequency* ID), que são anexados às mensagens de dados de medição que são transmitidas, com alta e baixa periodicidade respectivamente, do medidor para a concessionária de energia. As mensagens que têm uma baixa periodicidade de transmissão carregam consigo dados de gerenciamento de conta e faturamento, enquanto as

mensagens que têm uma alta periodicidade são aquelas que carregam informações sobre os padrões de uso dos aparelhos elétricos, essas últimas que deverão ser protegidas. Para isso, se fez necessário que apenas um serviço terceirizado confiável soubesse os pares HFID-LFID de cada medidor inteligente. As mensagens com informações privadas seriam reconhecidas, portanto, apenas pelo serviço terceirizado e não mais fariam sentido para as distribuidoras, já que não saberiam de qual medidor aquelas informações se originaram. Além disso, os autores propõem perfis de operação para medidores inteligentes, *Client Data Profile* (CDP) e *Anonymous Data Profile* (ADP), e descrevem seus fluxogramas de comunicação para uma configuração inicial. Diferentemente, nossa proposta não garante a privacidade dos dados de consumo, mas sim a confiabilidade, não-repúdio e integridade dos mesmos.

Em Treytl *et al.* (TREYTL *et al.* 2004), é descrita uma arquitetura de segurança, chamada REMPLI (*Real-time Energy Management via Power lines and Internet*), com o objetivo de prover autenticação e integridade dos dados na comunicação via PLC (*Power Line Communication*) entre os medidores dos consumidores e os serviços SCADA (*Supervisory Control and Data Acquisition*) das empresas concessionárias de energia. Os autores levantam ameaças e riscos relacionados a cada camada de segurança necessária para as operações e trocas de mensagens entre os dispositivos da arquitetura. Além disso, justificam o uso de um *smartcard* para fins de armazenamento seguro, manipulação e distribuição de chaves criptográficas. Por fim, realizam testes preliminares de desempenho de autenticação e encriptação com diferentes algoritmos de criptografia, e concluem, do ponto de vista do *overhead* de processamento da criptografia e do tamanho dos dados transmitidos via PLC, quais algoritmos simétricos com blocos de tamanho pequeno são mais eficientes. Além de garantir a integridade e a autenticidade dos dados gerados pelo medidor, a nossa solução propõe a assinatura digital dos dados de consumo no início da cadeia de medição, garantindo o não-repúdio destes dados e a rastreabilidade de qualquer alteração, maliciosa ou não, ocorrida posteriormente ao momento da assinatura.

Outras soluções de segurança para os medidores inteligentes estão sendo propostas fazendo o uso de módulos criptográficos integrados à arquitetura de medição. Em Feller *et al.* (FELLER *et al.* 2011), uma versão compacta do TPM (*Trusted Platform Module*) é implementada, a qual consume poucos recursos e requer um conjunto mínimo de comandos. Este módulo criptográfico é integrado ao medidor e provê proteção de propriedade intelectual, corretude do comportamento e atualização segura do *software*. Em outro projeto, a Infineon, uma fabricante de semicondutores, desenvolveu a família de *chipset* UMF11x0 (INFINEON

2012) para medidores inteligentes que pode ser conectados a um *smartcard* ou a um módulo de segurança de *hardware* (HSM). Esse chip oferece funções para criptografia simétrica (AES-128/256) e para uma Infraestrutura de Chave-Pública, além de proteção das chaves criptográficas e um gerador de números aleatórios reais.

Apesar dos trabalhos citados anteriormente apontarem preocupações e soluções sobre a segurança e corretude do comportamento dos medidores inteligentes, o trabalho nesta dissertação é o primeiro a propor uma arquitetura de segurança que disponibiliza um procedimento prático de verificação de integridade dos dados gerados por um medidor inteligente e capaz de ser realizado por um usuário comum.

Em relação ao uso de assinaturas digitais com restrição de tamanho, o trabalho de Naccache e Stern (NACCACHE e STERN 2000) investiga meios de assinar digitalmente pequenas mensagens usando um esquema de assinatura que minimiza o tamanho total da mensagem original e do *overhead* criptográfico. A motivação é dada pelo advento do serviço de *Internet Postage*, onde o usuário é capaz de imprimir um selo postal para sua própria correspondência, onde o selo postal é composto pelas informações do destinatário, data e tempo e uma assinatura digital codificadas em uma *2-D barcode*. Essa assinatura digital, no entanto, deverá ser pequena sem gastar muito do limitado espaço. O trabalho propõe um esquema de assinatura digital variante ao ECDSA que permite recuperação de mensagem parcial e, por fim, descreve duas possíveis otimizações, avaliando seus custos em termos de gastos de memória e de tempo.

Em Yavuz *et al.* (YAVUZ *et al.* 2006) é proposto um protocolo de segurança *multicast* de satélite baseado no esquema de assinatura digital ECPVS. Para uma abordagem em um ambiente de banda de comunicação limitada, o ECPVS é usado para assegurar a chave de grupo e transmissão da semente, além de prover métodos eficientes de confidencialidade.

Em Freitas *et al.* (FREITAS *et al.* 2009) é apresentado um solução para a implementação de uma assinatura digital compacta e segura, como parte integrante do projeto "Selo Verde" da Universidade de São Paulo. Os autores desenvolvem a proposta da assinatura sobre os seguintes requisitos semelhantes ao presente trabalho: (**i**) compacta, usando o menor número de caracteres possíveis devido ao espaço restrito da etiqueta do projeto, (**ii**) reconhecíveis e legíveis, a leitura do código deverá ser feita por qualquer pessoa sem necessidade de qualquer aparelho específico e (**iii**) publicamente verificáveis em aparelho comum, será possível em qualquer computador que tenha acesso ao site de verificação. O

conceito foi criado utilizando assinaturas BLS (BONEH *et al.* 2001) e verificação de redundância cíclica, o CRC-4.

3.1 Conclusão

Este capítulo apresentou trabalhos relacionados com o tema desta dissertação. Descrevemos os principais documentos existentes que servem como guias para avaliação de conformidade dos modelos de instrumentos de medição, assim como é abordada a questão da segurança da informação na infraestrutura de distribuição de energia na Alemanha.

Em seguida, foram apresentados artigos que propõe soluções e arquiteturas de segurança para as questões gerais de segurança da informação envolvendo os medidores inteligentes. Por fim, incluímos alguns projetos que utilizam de alguma forma, assinaturas digitais com restrições de tamanho devido às limitações existentes de cada ambiente em questão.

4 Arquitetura de Segurança para Medidores Inteligentes

Nesta seção são descritos: (**i**) a abordagem proposta pelo arcabouço de segurança para a validação da medição, (**ii**) os objetivos do projeto e seus requisitos atendidos, (**iii**) as modificações propostas na arquitetura do medidor inteligente para implantação da arquitetura de segurança, (**iv**) o Módulo de Medição Confiável (TMM), (**v**) o Processo de Verificação da Medição e (**vi**) o Autenticador de Consumo Distribuído por Hora.

4.1 Abordagem Proposta

Uma **arquitetura de segurança** é um conjunto de procedimentos, ações, recursos e soluções para atender às preocupações de segurança. A proposta deste trabalho é a concepção de uma arquitetura de segurança que estabeleça **confiabilidade nos dados gerados** pelo medidor inteligente para todas as partes interessadas – o consumidor, a concessionária de energia elétrica e a autoridade metrológica. A arquitetura é composta por mecanismos de segurança, como criptografia de chave-pública e assinatura digital, juntamente a procedimentos externos de verificação de dados.

Como base para toda a segurança provida, introduziremos um esboço de um dispositivo de *hardware* que atuará como "raiz de confiança" da arquitetura aqui apresentada. A este dispositivo daremos o nome de **Módulo de Medição Confiável**, ou **TMM** (sigla de *Trusted Metering Module*). O TMM é um módulo criptográfico acoplado ao início da cadeia de medição, localizado no módulo de medição, com o objetivo de armazenar dados referentes à energia consumida e repassá-los à frente, para o resto da cadeia de medição, assinados digitalmente. Demais características e funcionalidades do módulo são descritos na seção 4.3.

Os dados acumulados de energia consumida assinados em um determinado instante serão a base para compor um autenticador de consumo. A esse autenticador, atribuiremos o nome **Autenticador de Consumo Distribuído por Hora** (ACD). O Autenticador de Consumo Distribuído por Hora constitui uma sequência alfanumérica que deverá ser disponibilizada no visor do dispositivo mostrador e atualizada juntamente com cada atualização de valores de consumo (Figura 5). Segundo a Portaria Inmetro nº 11 de 2009, o tempo máximo permitido de atualização dos dados no visor do dispositivo mostrador para cada kWh consumido é de 60 segundos.

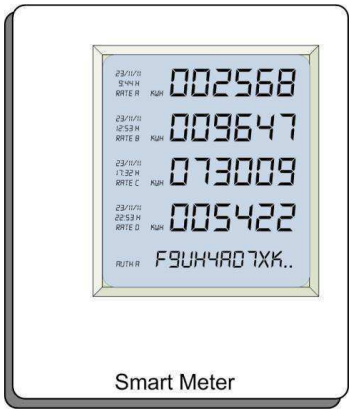

Figura 5. Exemplo de um Dispositivo Mostrador com 4 valores de kWh acumulado por posto tarifário e o Autenticador de Consumo Distribuído por Hora.

Dessa maneira, o autenticador ACD torna-se um meio para que consumidor possa verificar se os valores de consumos exibidos estão, de fato, autenticados (a origem dos dados pertence ao módulo de medição correto) e íntegros (os dados não sofreram alterações). O autenticador ACD será descrito detalhadamente na seção 4.5.

Para realizar essa verificação, o consumidor poderá então iniciar o **Processo de Verificação da Medição** (PVM). Basicamente, o PVM consiste na transcrição do autenticador ACD e os valores de consumo de energia exibidos em um dado instante pelo dispositivo mostrador, e a inserção destes em um sistema computacional. Esse sistema é, portanto, capaz de responder se o ACD é válido e, se ratifica ou não, os valores de consumo exibidos. Mais detalhes sobre o Processo de Verificação da Medição e os dados de entrada necessários para a sua realização serão descritos na seção 4.4.

Na Figura 6, podemos visualizar o funcionamento da arquitetura de segurança de forma ilustrada. O quadro (**a**) apresenta um cenário comum da utilização do Sistema Distribuído de Medição de Energia Elétrica (SDMEE) no Brasil, onde um Concentrador Secundário encontra-se localizado no topo de um poste de luz, enquanto, na residência do consumidor, um Dispositivo Mostrador exibe os valores de consumo de energia. O quadro (**b**) destaca a cadeia de medição existente em um dos módulos de medição do Concentrador Secundário e indica o fluxo de dados de consumo a serem assinados digitalmente: a entrada no módulo TMM, a geração de um autenticador ACD, e seu repasse à aplicação/*firmware* do fabricante. Em seguida, no quadro (**c**), o módulo de medição comunica a atualização de dados de consumo, juntamente com seu autenticador ACD correspondente, ao seu Dispositivo Mostrador correspondente. Por fim, o quadro (**d**) destaca o Dispositivo Mostrador e exemplos de destinos dos dados que constam no visor para a realização do PVM. No exemplo, o PVM

pode ser realizado em um sistema *desktop*, ou no *website* da autoridade metrológica, ou pela concessionária de energia elétrica.

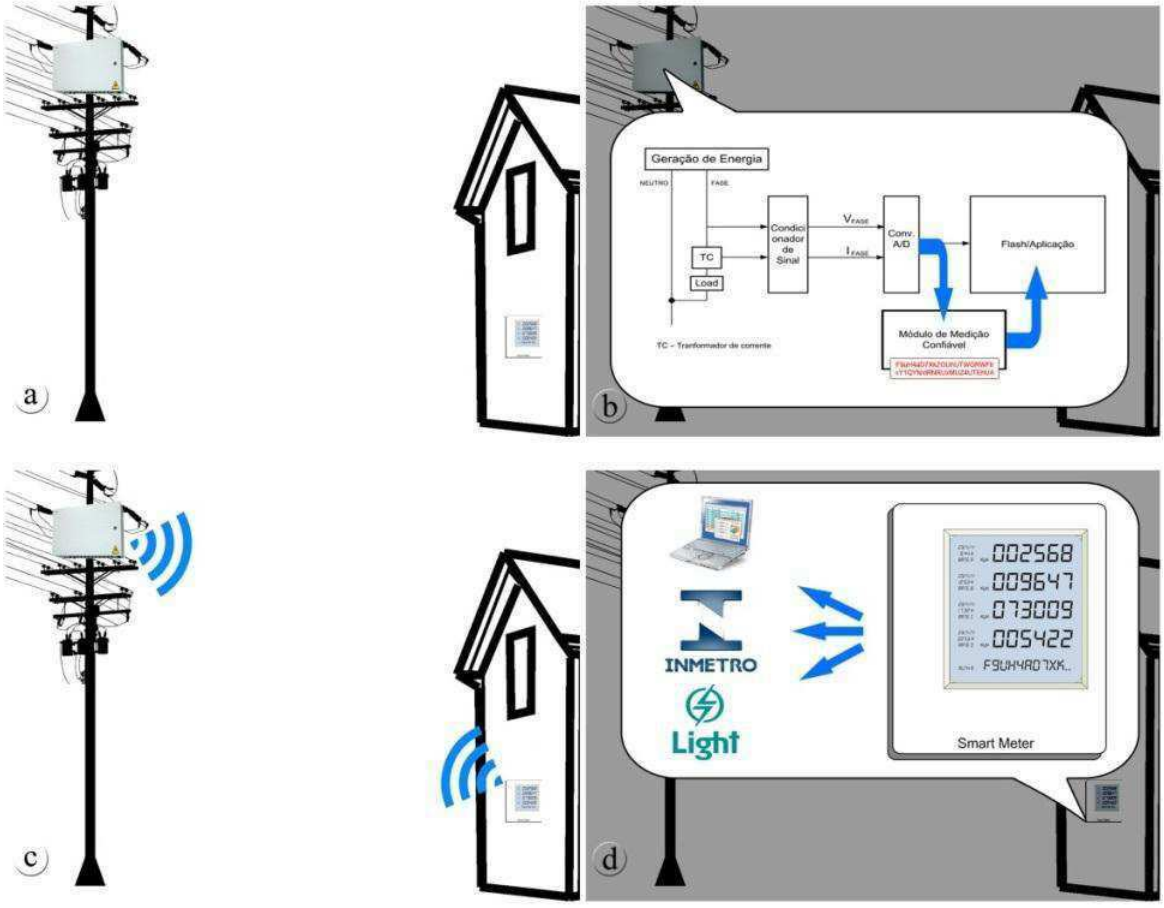

Figura 6. Etapas do funcionamento da arquitetura de segurança proposta.

4.2 Objetivos e Requisitos do Projeto

Nesta subseção, reafirmamos os objetivos almejados com a arquitetura de segurança para medidores inteligentes proposta, além de detalhar os requisitos específicos deste projeto. Abaixo, seguem os objetivos em mente:

- Reduzir o esforço empregado durante o processo de aprovação de modelos de medidores inteligentes, introduzindo uma alternativa à análise completa de código-fonte;
- Prover confiança no comportamento do medidor inteligente para as partes interessadas, garantindo a autenticidade e integridade dos dados de consumo.

Durante o processo de aprovação de modelos de medidores, a autoridade metrológica **restringiria sua análise apenas aos componentes legalmente relevantes** (definido na seção

2.2) **que se encontram antes do TMM** na sequência da cadeia de medição, uma vez que seria apenas necessário garantir que os dados de entrada do TMM sejam genuinamente dos sensores de corrente e voltagem. Dessa forma, o TMM garante a rastreabilidade dos dados originais. Como consequência do uso dessa arquitetura, a autoridade metrológica **mitigaria os riscos de vazamento de propriedade intelectual** associados à abertura e armazenamento do código-fonte da aplicação metrológica dos fabricantes de medidores.

Em relação ao segundo item, através do Autenticador de Consumo Distribuído por Hora e do Processo de Verificação da Medição, os consumidores terão meios de estabelecer confiança nos dados de consumos exibidos no visor e cobrados em sua conta de luz. Para as distribuidoras de energia elétrica, sua confiança nos medidores inteligentes em operação também aumenta, uma vez que elas poderão recuperar os autenticadores ACD remotamente e atestar se seus medidores sofreram algum tipo de violação que comprometa a integridade de seus dados.

Em adição aos objetivos gerais, seguem abaixo os objetivos específicos estipulados para este projeto e os comentários sobre cada um deles:

1. Estabelecer as mudanças necessárias na arquitetura de um medidor inteligente, priorizando a mitigação de vulnerabilidades;
2. Especificar uma solução de segurança que suporte diferentes cenários de multitarifação de energia, isto é, diferentes modalidades de Postos Tarifários (*Time-Of-Use*);
3. Especificar uma solução de segurança que possua custos de funcionamento reduzidos;
4. Estabelecer maneiras de compor um autenticador de consumo.

O projeto da arquitetura de segurança é orientado, mas não restrito, à arquitetura do Sistema Distribuído de Medição de Energia Elétrica (SDMEE), previamente descrita na seção 2.2.1. A razão dessa escolha é respaldada pelo fato de que o SDMEE é um sistema que está sendo amplamente adotado pelos fabricantes de medidores que disputam o mercado brasileiro, tendo que se adequar às normas do Inmetro. Do primeiro objetivo específico, é prevista a inserção de um novo dispositivo de *hardware* na arquitetura do SDMEE, atuando como “raiz de confiança”. Essa “raiz de confiança” deverá ter seu posicionamento especificado e interação restrita com os demais dispositivos. Dessa forma, pretendemos

minimizar ao máximo as possibilidades de *backdoors* na "raiz de confiança". Mais detalhes serão vistos na seção 4.3.

Sobre o segundo objetivo específico, a arquitetura de segurança aqui proposta foi desenvolvida para **dar suporte às novas práticas de multitarifação de energia** durante diferentes períodos do dia, os chamados Postos Tarifários, atualmente aplicados em diversas regiões do mundo. Ademais, a arquitetura atua **independentemente da modalidade de tarifação** e configuração dos postos estipulada pelas distribuidoras de energia, consequentemente podendo ser adotada por diferentes distribuidoras e em diferentes regiões.

A arquitetura de segurança oferece meios de não apenas verificar o consumo total exibido pelo medidor inteligente, mas verificar também os valores de consumo de energia nos diferentes postos tarifários estipulados pela modalidade tarifária em vigor. Os reflexos desse requisito no módulo TMM e no autenticador ACD serão vistos detalhadamente nas seções em sequência.

Através do terceiro objetivo específico pretende-se não onerar o custo de um medidor inteligente, nem dos procedimentos externos necessários para a verificação dos dados de consumo. Dessa forma, além do módulo TMM requerer recursos mínimos de armazenamento e funcionalidades, é mandatório no projeto que não haja necessidade de um segundo dispositivo comunicar-se com o medidor para possibilitar o Processo de Verificação da Medição. Logo, a leitura e transcrição dos dados de consumo e do autenticador ACD deverá ser possível e factível de forma manual, utilizando como meio o visor do dispositivo mostrador.

Como consequência do quarto objetivo específico, um dos estudos apresentados nesta dissertação é de que forma compor o autenticador de consumo e quais dados são necessários para isto, atentando para os requisitos necessários. Abaixo, especificamos os requisitos que o autenticador de consumo deverá atender:

1. Conteúdo da mensagem contida no autenticador: a mensagem deve conter informações necessárias a fim de validar os valores de consumo exibidos por Postos Tarifários;
2. Segurança do autenticador: o autenticador de consumo deve ser a prova de falsificações;
3. Tamanho do autenticador: o autenticador deverá conter um número apropriado de caracteres, capaz de tornar a sua transcrição manual viável;

4. Tempo de verificação do autenticador: o algoritmo de verificação, durante o Processo de Verificação da Medição, deverá executar e responder, em média, em menos de 60 segundos;

Uma vez que o mecanismo de segurança não tem conhecimento da configuração dos postos tarifários (horário de início e fim de cada posto), o conteúdo da mensagem contida no autenticador deve representar os valores consumidos de alguma forma. Caso os valores de consumo sejam alterados maliciosamente, as informações incluídas nesta mensagem permitem que isso possa ser detectado.

O ponto crítico reside no fato de que o autenticador de consumo deve prover segurança e completude de dados necessários para validação dos valores de consumo, por outro lado, deverá apresentar um número apropriado de caracteres e ainda ser capaz de oferecer um alto nível de acurácia e segurança contra falsificações para a informação que carrega, permitindo ainda uma transcrição prática e diminuindo as chances de erro manual durante o PVM. Algumas técnicas de composição do conteúdo do autenticador ACD são descritas e testadas no capítulo 5.

4.3 Módulo de Medição Confiável (TMM)

O Módulo de Medição Confiável, ou TMM, referente à *Trusted Metering Module*, é um módulo criptográfico capaz também de contabilizar e armazenar valores de energia consumida, além de possuir funcionalidades de sincronização de relógio e manipulação de dados, vistos no capítulo 5. O módulo atuará como "raiz de confiança" ("*root of trust*") para a arquitetura de segurança proposta. Neste trabalho, apresentamos um esboço desse módulo, onde suas principais características e recursos são identificados e colocados.

Os recursos de *hardware* do módulo TMM são: (**i**) o processador, (**ii**) o código do programa, o qual inclui as técnicas de composição do autenticador ACD, (**iii**) o motor de execução, responsável por "rodar" o código do programa e tratar os dados e comandos de entrada e saída do módulo, (**iv**) a memória protegida, para a guarda de chaves criptográficas, (**v**) a memória não-volátil, que armazena variáveis e registradores com valores de energia consumidos, (**vi**) o motor de criptografia e assinatura digital, (**vii**) o motor de *hash* e (**viii**) o *Real Time Clock*, RTC. A Figura 7 ilustra os componentes internos do TMM.

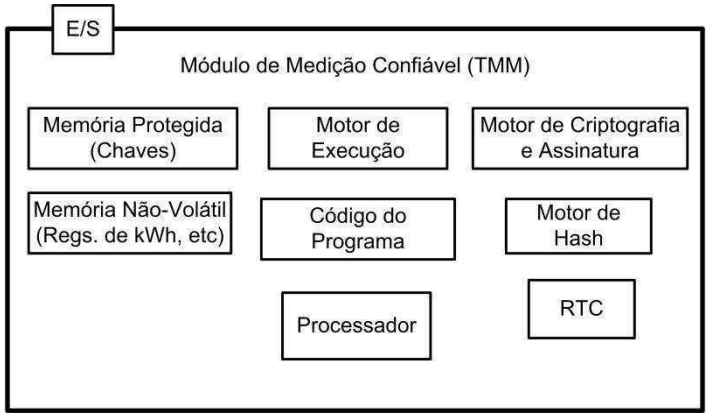

Figura 7. Diagrama de Bloco dos componentes internos do Módulo de Medição Confiável (TMM).

O módulo TMM tem como principais funções a manipulação e armazenamento seguro de dados relativos à energia consumida em kWh – a partir dos dados provenientes dos sensores de corrente e voltagem do medidor – com a finalidade de geração de um autenticador de consumo com dados íntegros e autenticados sobre os valores do consumo de energia. Para isso, o TMM contabiliza a energia consumida paralelamente à aplicação do módulo de medição do medidor e assina digitalmente esses dados.

Em sua memória protegida, o módulo TMM armazena uma chave-privada única, juntamente com sua chave-pública. A chave-privada deve ser gerada em tempo de fabricação e gravada no TMM obedecendo a critérios rígidos de segurança para evitar cópia e/ou vazamento dessas chaves. Para fins de verificação da autenticidade da assinatura de um TMM, um certificado digital deverá ser criado para ele. O certificado digital é usado de forma a atrelar a identificação do módulo TMM a sua chave-pública, endossado por uma Autoridade Certificadora e integrante de uma Infraestrutura de Chaves Públicas confiável. No caso brasileiro, a autoridade deverá ser integrante da ICP-Brasil (Infraestrutura de Chaves Públicas - Brasil).

Em relação à mitigação de possíveis vulnerabilidades e *backdoors*, o módulo TMM mantém um número mínimo de entradas necessárias de dados. As duas entradas de dados do módulo referem-se: (**i**) aos dados das grandezas de voltagem e corrente, provenientes das fases do circuito elétrico da instalação, amostrados por um Conversor Analógico/Digital e (**ii**) aos comandos para correção/sincronização do RTC, localizado no TMM, juntamente ao relógio da aplicação do fabricante. Essa sincronização é de responsabilidade da aplicação do fabricante.

A sincronização entre o relógio da aplicação e o RTC do módulo TMM é fundamental para que o módulo atue corretamente, inclusive no período do horário de verão. No entanto, a livre sincronização do RTC pela aplicação do fabricante permitiria ataques às operações do módulo TMM. Como um exemplo de ataque, a aplicação poderia sincronizar o RTC nos períodos de início e término dos postos tarifários a fim de "alongar" o período de pico e, assim, contabilizar mais consumo de energia durante o período mais caro. A fim de desencorajar essa prática maliciosa, um protocolo de sincronização do RTC do módulo TMM precisa ser elaborado. Apesar da formalização desse protocolo estar fora do escopo desta dissertação, destacamos alguns pontos de funcionamento da seguinte forma: a sincronização do RTC poderá acontecer até um número máximo de vezes ao ano, aliado ao fato de que todos os detalhes relacionados ao evento de sincronização necessitam ser registrados em *log* interno ao módulo, garantindo a rastreabilidade de qualquer alteração. Além disso, como um quesito adicional, a sincronização deverá ser feita na primeira hora do dia, que normalmente se trata de um período fora-de-pico, evitando que aplicações maliciosas alonguem o período de tarifação mais cara.

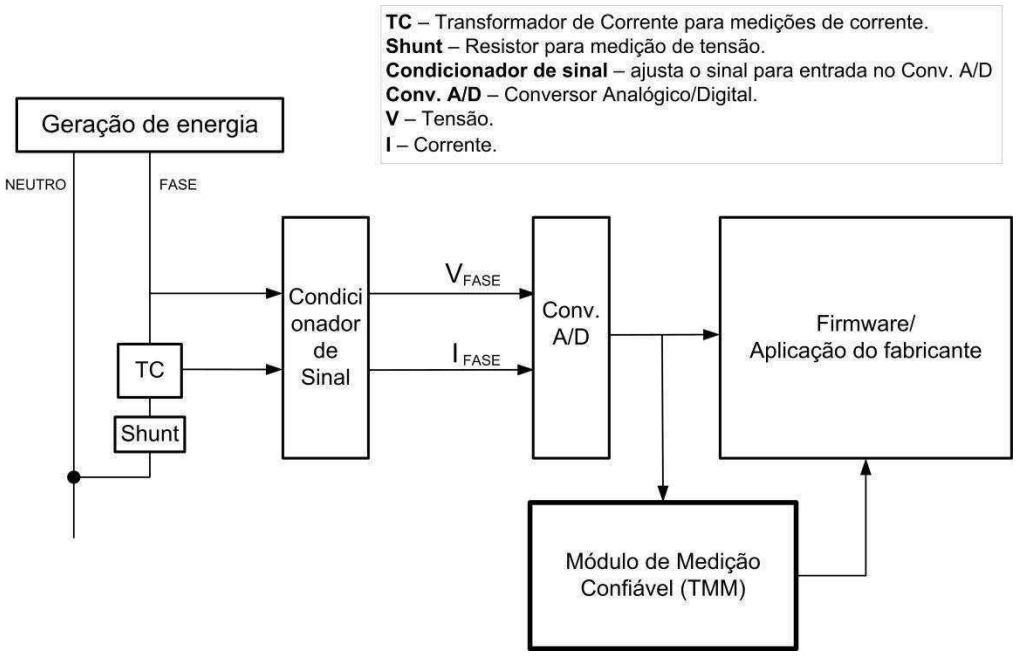

Figura 8. Diagrama de Bloco dos componentes de um módulo de medição e localização do Módulo de Medição Confiável (TMM).

Em relação a sua posição na arquitetura do módulo de medição do medidor inteligente, o TMM deve ser acoplado o mais próximo possível do início da cadeia legalmente relevante de medição (). Ele deverá estar obrigatoriamente localizado na cadeia de medição antes da aplicação do fabricante e após o conversor Analógico/Digital que amostra as grandezas de

medição. É possível que, em alguns modelos de medidores inteligentes, esse conversor Analógico/Digital já esteja integrado no microcontrolador do módulo de medição, sendo assim, necessária a adição de outro conversor Analógico/Digital para servir as entrada de dados ao TMM.

O *Real Time Clock*, por sua vez, tem como finalidade prover ao TMM o horário correto e sincronizado com a aplicação do fabricante. Assim como nos medidores TOU que compreendem funcionalidades de multitarifação de energia e necessitam registrar o consumo de energia em períodos pequenos, o RTC usado deve ser bem preciso, com erro abaixo de 5 ppm (partes por milhão) (ARORA 2011), o que representa um erro inferior a 2 minutos ao ano. Logo, a partir das duas entradas de dados mencionadas, o módulo TMM é capaz de calcular e armazenar adequadamente os valores de consumo de energia.

De fato, o módulo TMM "desconhece" a configuração de tarifação realizada pela concessionária de energia, isto é, ele não sabe determinar o início/término dos postos tarifários. Portanto, o módulo deve lidar com a tarifação horo-sazonal de energia da forma descrita na sequência. O TMM contabiliza em registradores os dados de energia consumida em kWh por períodos fixos de uma hora de duração, iniciando sempre na virada da hora. Existem, portanto, 24 registradores armazenando valores acumulados de consumo desde o tempo de instalação do medidor até o momento presente. Cada registrador mantém o valor consumido durante o período de uma determinada hora do dia (por exemplo, Registrador 0 – 00:00:00 às 00:59:59h, Registrador 18 – 18:00:00h às 18:59:59h).

Além desses 24 registradores de valores de consumo acumulado por hora, três registradores extras serão reservados para armazenar os valores de consumo acumulados de todos os sábados, domingos e feriados nacionais respectivamente. Esses registradores extras são necessários uma vez que esses dias são cobrados de forma diferenciada dos dias úteis na maioria das modalidades de tarifação horo-sazonal existentes. Os fins-de-semana e feriados nacionais geralmente são classificados como períodos fora-de-pico.

Para que a identificação dos dias-de-semana e feriados seja possível, uma rotina de calendário deve integrar o código do programa do módulo TMM. A partir dessa rotina, o programa poderá identificar os dias da semana e feriados nacionais previstos em lei e contabilizar o consumo de energia no registrador correspondente.

Os valores de consumo armazenados em cada registrador são calculados como dados de kWh em função das grandezas de corrente e tensão originadas dos sensores do módulo de

medição. De fato, o módulo TMM não usa a chamada "função de medição" exatamente igual a que se encontra na aplicação do medidor, já que esta é propriedade intelectual do próprio fabricante do medidor inteligente. Para resolver isso, o TMM realiza os cálculos com uma função de medição própria e, durante o Processo de Verificação da Medição, é realizada uma correção entre as funções de medições do módulo e do fabricante.

Por fim, a única saída de dados do módulo TMM será direcionada à aplicação do módulo de medição. Para cada 1 kWh calculado e consumido pela unidade consumidora, o TMM repassará o autenticador ACD atualizado para a aplicação do fabricante.

4.4 Processo de Verificação da Medição

O Processo de Verificação da Medição é iniciado através da recuperação dos valores de consumo em kWh e o autenticador ACD correspondente a esses valores. Para o consumidor, o processo de recuperação é feito manualmente – lendo e transcrevendo esses dados da conta ou do visor do dispositivo mostrador – atendendo ao requisito da arquitetura de segurança da não necessidade de um segundo dispositivo para leitura dos mesmos. Já para a concessionária de energia elétrica, esses valores poderão ser recuperados remotamente através da conexão bidirecional, prevista no conceito de medidores inteligentes.

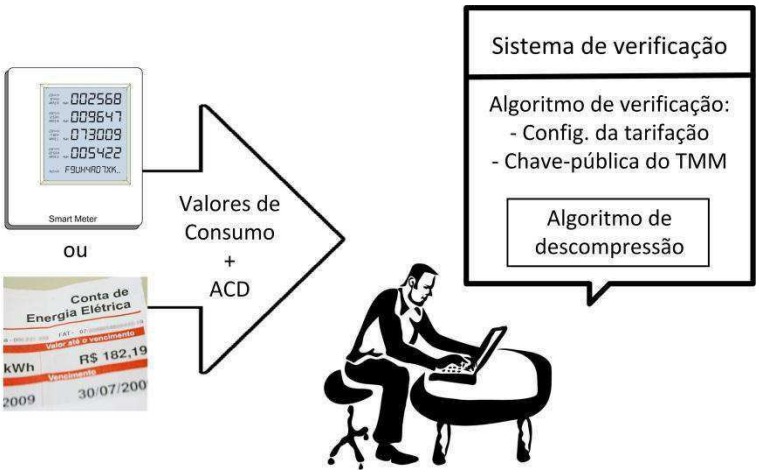

Figura 9. O Processo de Verificação da Medição pelo consumidor.

Uma vez que esses dados estejam recuperados, eles são inseridos como entrada de um sistema computacional, este podendo ser uma página *web* ou aplicativo *desktop*, homologado pela Autoridade Metrológica Legal (no caso brasileiro, o Inmetro). O sistema espera as seguintes informações como entrada de dados (Figura 9):

a. Valores de consumo da unidade consumidora por posto tarifário (Ex: Posto 1 – 2500 kWh, Posto 2 – 3800 kWh, etc.)

b. O Autenticador de Consumo Distribuído por Hora correspondente.

Além disso, o sistema de verificação deverá ter acesso a, ou permitir também como entrada, as seguintes informações:

c. Horários de início e fim de cada posto tarifário da modalidade de tarifação em que opera o medidor inteligente a ser verificado.

d. Chave-pública, ou Certificado Digital, correspondente ao módulo TMM do medidor a ser verificado.

Após a submissão e processamento desses dados, o sistema enfim poderá atestar a corretude dos valores de consumo exibidos, respondendo “Sim”, para dados válidos, ou “Não”, caso contrário.

O algoritmo de verificação do PVM deverá contar com uma função capaz de realizar a correção dos valores de saída da função de medição localizada no TMM para valores de saída da função de medição do fabricante do medidor. Essa função de correção varia de fabricante para fabricante, uma vez que cada um calcula de maneira particular o consumo final de kWh consumidos.

4.5 Autenticador de Consumo Distribuído por Hora (ACD)

O Autenticador de Consumo Distribuído por Hora, ACD, é o meio pelo qual a arquitetura de segurança proposta disponibiliza dados necessários sobre o consumo do medidor inteligente ao usuário interessado em verificar seu comportamento, em meio a um cenário de tarifação horo-sazonal.

Para o consumidor, o autenticador ACD é disponibilizado, como uma sequência alfanumérica, no visor do dispositivo mostrador para consulta instantânea. Para a concessionária de energia elétrica, o autenticador poderá ser recuperado remotamente através da comunicação de dados existente entre ela e o medidor inteligente e, oportunamente, usado também para verificação do equipamento ou ainda incluído na conta de luz do seu cliente, adicionando confiabilidade aos valores de consumo cobrados.

Tecnicamente, o ACD é uma assinatura digital que permite recuperação de mensagem. Ou seja, além de a assinatura garantir a origem e integridade de determinados dados, esses mesmos dados, ou parte deles, poderão ser criptografados e embutidos na assinatura digital.

A característica desse mecanismo atende o papel esperado do autenticador ACD, pois, dessa maneira, os dados provenientes do TMM poderão ser externalizados e validados de maneira segura, a salvo de falsificações. Caso haja algum tipo de modificação no código que representa o ACD, isso será detectável, quando ele for verificado, e invalidará o autenticador. Por fim, caso o ACD esteja válido, a mensagem contida nele poderá ser recuperada de forma íntegra e usada no Processo de Verificação da Medição.

O esquema de assinatura digital escolhida para o autenticador ACD será o ECPVS – *Elliptic Curve Pintsov-Vanstone Signature* – adotada em diversas normas, incluindo IEEE P1363a, ANSI X9.92 e ISO 9796-3 (ISO/IEC 2006). O ECPVS é um esquema com recuperação parcial de mensagem baseado em ECC (*Elliptic Curve Cryptography*). Ela foi projetada para ser a prova de falsificações, mesmo na presença de um adversário capaz de produzir ataques por texto escolhido (CERTICOM 2011). Essa característica de segurança é importante para evitar futuras falsificações do ACD pelo aplicativo do fabricante no medidor, e que poderia ser realizada como um exemplo de ataque descrito em seguida. Um criptoanalista, a serviço do fabricante ou concessionária de energia, realizaria tentativas de derivar/descobrir a chave-privada única do módulo TMM usada na assinatura, através de um conjunto de ACDs gerados pelo TMM. Ao obter sucesso, essa chave-privada seria, então, carregada e armazenada pelo aplicativo do medidor inteligente. Logo, desse instante em diante, o medidor malicioso descartaria os ACDs provenientes do módulo TMM e usaria essa chave armazenada para gerar seus próprios autenticadores.

A geração de autenticadores falsificados se torna possível quando o aplicativo do medidor malicioso sabe, além da chave-privada de seu TMM correspondente, compor adequadamente a mensagem embutida no ACD. Portanto, uma vez que os dados necessários para montar a mensagem são os dados de medição e as técnicas de composição desta mensagem são públicas, um código malicioso poderia facilmente gerar autenticadores falsificados válidos.

No caso do ataque descrito acima, ele seria viabilizado pelo criptoanalista somente por um ataque de texto conhecido (*known plaintext*), pois a mensagem embutida na assinatura é pública. No entanto, esse tipo de ataque possui ainda menos chances de sucesso do que um ataque de texto escolhido (*chosen plaintext*) (STALLINGS 2006).

Outra característica do esquema ECPVS, e a mais pertinente para esse projeto, é que esse esquema fornece uma assinatura digital de tamanho menor frente a outros esquemas mais comuns de assinatura. Para fins de exemplificação, uma típica assinatura ECDSA (*Elliptic Curve Digital Signature Algorithm*), usando uma curva de 160 bits sobre conjuntos finitos primos, é um apêndice de 40 bytes adicionado a uma mensagem assinada. Por outro lado, uma assinatura equivalente usando RSA adicionaria um *overhead* criptográfico de 128 bytes. No mesmo nível de segurança, uma assinatura ECPVS adicionaria apenas 20 bytes ao comprimento da mensagem original (CERTICOM 2004).

Dessa forma, a assinatura ECPVS fornece um tamanho de *overhead* criptográfico razoavelmente adequado para uma leitura humana utilizando-se algum tipo de codificação padrão para texto. Para o presente trabalho, convencionou-se usar a codificação base64 para representação da assinatura.

No esquema ECPVS, a assinatura contém duas partes, *r* e *s*. O comprimento da segunda parte, *s*, está diretamente relacionado ao tamanho da chave-privada usada para assinar. Já o comprimento da primeira parte, *r*, é basicamente em função do tamanho da parcela da mensagem que se deseja recuperar posteriormente. No autenticador ACD, a parcela da mensagem recuperável é a mensagem completa, ou seja, não haverá mensagem em claro (texto compreensível) junto à assinatura.

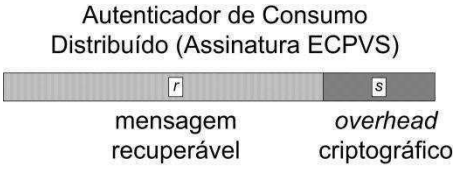

Figura 10. Ilustração de um ACD (assinatura ECPVS).

Portanto, temos uma mensagem que será embutida na assinatura digital e, a partir dela, os dados gerados pelo módulo TMM poderão ser analisados e confrontados com os valores de consumo do visor. No entanto, essa característica levanta algumas questões a serem respondidas em seguida: que mensagem é esta que será embutida? Como compor esta mensagem? E como minimizá-la para que o autenticador ACD possa conter um número razoável de caracteres? Os detalhes das técnicas de composição do ACD se encontram no próximo capítulo.

4.6 Conclusão

Este capítulo apresentou a arquitetura de segurança para medidores inteligentes proposta neste trabalho. Primeiramente, foi descrita uma visão geral do funcionamento, mecanismos e procedimentos externos que integram a arquitetura. Em seguida, relembramos os objetivos gerais e específicos esperados com a implementação dessa arquitetura de segurança e os requisitos do autenticador de consumo que precisam ser atendidos.

Apresentamos um esboço do Módulo de Medição Confiável (TMM) como a “raiz de confiança” da arquitetura, assim como suas principais características. Em seguida, o Processo de Verificação da Medição foi abordado, descrevendo como ele deve ser realizado e quais dados de entrada do algoritmo de verificação são necessários. Por fim, detalhamos o Autenticador de Consumo Distribuído por Hora, sua estrutura e justificamos a escolha do esquema de assinatura ECPVS.

5 Técnicas para Composição do Autenticador de Consumo

Nesta seção são descritos: (**i**) os parâmetros de domínio e premissas do volume de dados consideradas para a construção do Autenticador de Consumo Distribuído por Hora, (**ii**) as técnicas usadas para composição da mensagem embutida no autenticador e (**iii**) a análise experimental de cada técnica e os resultados obtidos. Por fim, serão apresentadas (**iv**) duas abordagens alternativas de autenticador: o Autenticador Relativo e o Autenticador de Consumo por Postos Tarifários.

5.1 Introdução

Essa seção apresenta quatro técnicas desenvolvidas para composição da mensagem embutida no autenticador ACD, a qual, a partir de agora, chamaremos "**mensagem-ACD**". As técnicas especificam como os dados contidos na mensagem-ACD são estruturados e apresentam redundância, característica essencial para garantir a integridade de uma mensagem recuperada de uma assinatura ECPVS (CERTICOM 2011).

A mensagem-ACD deve conter dados suficientes para ser possível validar os valores de consumo em kWh em cada faixa de preço. Uma vez que o módulo TMM não tem conhecimento sobre os postos tarifários definidos, a mensagem-ACD representará, de alguma forma, os valores dos registradores do TMM, tornando possível o Processo de Verificação da Medição.

Ademais, é desejável a **redução do comprimento da mensagem-ACD**, comprimindo os dados de forma a serem recuperáveis em sua totalidade. As técnicas atentam para o fato de que, quanto menor for o comprimento final da mensagem-ACD maior será o tempo de recuperação das informações nela contidas. A relação de compromisso (*trade-off*) entre comprimento da mensagem-ACD e o tempo para a recuperação das informações é estudada na seção 5.6, de avaliação das técnicas.

A primeira técnica não apresenta compressão, apenas uma organização dos dados necessários para a validação da medição. No entanto, as técnicas seguintes (Quantização Escalar, Contadores em Módulo e Contadores em Função de Dispersão) estabelecem maneiras particulares de representar os dados necessários para a realização posterior do Processo de Verificação da Medição.

Para estabelecimento do número de bits necessários para cada dado colocado na mensagem-ACD, consideramos as seguintes premissas:

- O **consumo mensal máximo** de uma residência: 4.000 kWh. Segundo Francisquini (FRANCISQUINI 2006), as unidades consumidoras no Brasil são divididas em classes de consumo. Essas classes dividem-se em (**i**) menor que 100 kWh/mês; (**ii**) entre 101 e 200 kWh/mês; (**iii**) entre 201 e 300 kWh/mês; (**iv**) entre 301 e 500 kWh/mês e (**v**) maior que 500 kWh/mês. Logo, estamos considerando um valor razoavelmente alto para que seja abrangida a grande maioria das diferentes classes residenciais de consumo.
- A **vida útil máxima** de operação de um medidor inteligente: 20 anos. Neste caso, também consideramos um valor razoavelmente alto, pois segundo Guimarães (GUIMARÃES 2006), a vida útil máxima de um medidor mecânico é de 15 anos, enquanto de um medidor eletrônico é de apenas 9 anos.

De acordo com os algoritmos de assinatura digital e funções de *hash* recomendados no *Federal Information Processing Standards Publications* publicado em NIST (2009), os **parâmetros de domínio** escolhidos para o processo de assinatura do ACD nas quatro técnicas apresentadas são:

1. Chaves baseadas em **curvas elípticas de 224 bits** sobre corpos finitos primos – aceita pelo NIST para geração e verificação de assinatura digital (BARKER e ROGINSKY 2011);
2. Função de *Hash*: **SHA-224** – aceita pelo NIST para todas as aplicações de função de *hash* (BARKER e ROGINSKY 2011);
3. Cifrador simétrico: **XOR Encryption Scheme** – usaremos o XOR como cifrador simétrico uma vez que não há real necessidade de confidencialidade da mensagem-ACD, no entanto, a previne de ataques passivos, adicionando uma camada fraca de confidencialidade (CERTICOM 2000).

Com as nossas premissas e os parâmetros de domínio estabelecidos acima, podemos introduzir as técnicas de composição da mensagem-ACD. Em seguida, simulamos os parâmetros referentes a cada técnica e concluímos o tamanho final do autenticador ACD para cada uma, como resultado dos testes da seção 5.6.

5.2 Técnica por Valores Absolutos

A Técnica por Valores Absolutos estabelece uma forma de organizar os dados necessários, originados do módulo TMM, a fim de uma posterior verificação. Nesse caso, nenhum tipo de processamento é realizado no dado e seus valores absolutos são colocados diretamente na mensagem.

Sejam os valores nos registradores do módulo TMM Val_i, para $i \in [0, 23]$, logo suas representações Rep_i na mensagem-ACD são determinadas pela Equação 1.

$$Rep_i = Val_i$$

Equação 1. Cálculo da representação Rep_i pela Técnica por Valores Absolutos.

De acordo com as premissas feitas na seção anterior, sobre consumo mensal máximo de uma residência e vida útil máxima de um medidor, o valor de Val_i não deverá ultrapassar 40.000 kWh. Logo, fixaremos $k = 16$, onde k é o número de bits necessários para Rep_i (podendo variar de 0 a 65.535) e compor a mensagem-ACD (mensagem recuperável) da seguinte maneira:

a. Soma dos períodos fora-de-pico (fins-de-semana e feriados): 20 bits;

b. As 24 representações dos registradores (Rep_0 - Rep_{23}): 16 bits para cada representação;

c. *Hash* dos 24 valores de cada registrador concatenados ($Hash_{abs}$): 32 bits (valor escolhido para fins de arredondamento durante a codificação base64);

A primeira parte da assinatura, chamada *r*, é onde a mensagem-ACD se localiza. A mensagem é o resultado da **concatenação das três sequências de bits** declaradas acima. A segunda parte da assinatura, *s*, será composta por um *overhead* criptográfico de 28 bytes (esperado de uma chave-privada ECC-224). Dessa forma, teremos uma assinatura (*r*, *s*) de comprimento final de 54,5 + 28 = **82,5 bytes**, o que em codificação base64 resultaria em **110 caracteres**. Esse comprimento necessita ser diminuído.

Como uma primeira manobra para reduzir o tamanho da assinatura, sugerimos que um rearranjo de dados seja realizado. Aos nossos conhecimentos, todas as modalidades existentes atualmente de multitarifação de energia consideram o período entre 23:00:00h - 5:59:59h da manhã como horário fora-de-pico. Assim sendo, poderemos somar todos os valores dos sete registradores correspondentes ao bloco de bits para períodos fora-de-pico (antes apenas reservado para fins-de-semana e feriados) e, dessa forma, reduzir o tamanho da mensagem-

ACD sem prejudicar o resultado final. Logo, com essa alteração, eis a nova composição da mensagem:

a. Soma dos períodos fora-de-pico (Val_{23} - Val_5, fins-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): 16 bits para cada representação;

c. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): 30 bits;

A nova mensagem-ACD é, portanto, a concatenação dos três itens acima, resultando um total de 322 bits. Dessa forma, o novo comprimento final da assinatura (r, s) será de 40,25 + 28 = **68,25 bytes**, gerando **91 caracteres** codificados em base64.

Com a Técnica por Valores Absolutos, essa é o menor tamanho do autenticador ACD (assinatura (r, s)) esperado. A seguir, são apresentadas as três técnicas considerando compressão lógica de dados.

5.3 Técnica por Quantização Escalar

A Técnica por Quantização Escalar estabelece um modo de representar os valores de consumo de cada registrador de hora dentro de um intervalo fixo de inteiros, equivalente a um processamento de sinal analógico para digital, incluindo perda de resolução. Porém essa perda pode ser recuperada posteriormente, como explicamos mais adiante.

Nesse novo método, o valor de um registrador i (Val_i), antes representado suficientemente por 16 bits (65.536 valores diferentes), será representado agora por k_{esc} bits ($2^{k_{esc}}$ valores diferentes) na mensagem-ACD, sendo $k_{esc} < 16$. Logo, analisamos que, com o passar do tempo e aumento do valor absoluto de consumo em cada registrador ultrapassando k_{esc}-1 unidades, suas representações na mensagem-ACD terão que ser escalados dentro do intervalo de inteiros [0, $2^{k_{esc}}$-1]. Seja Val_{maior} o maior valor entre todos os registradores, a representação do registrador i (Rep_i) será dada pela Equação 2.

$$Rep_i = \left\lfloor \frac{Val_i \times 2^{k_{esc}}}{Val_{maior} + 1} \right\rfloor$$

Equação 2. Cálculo da representação Rep_i pela Técnica por Quantização Escalar.

A composição da mensagem-ACD pela Técnica por Quantização Escalar compreende os seguintes dados:

a. Soma dos períodos fora-de-pico (Val_{23} - Val_5, fins-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): (17 × k_{esc}) bits;

c. O maior valor absoluto entre todos os registradores (Val_{maior}): 16 bits;

d. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): h_{esc} bits.

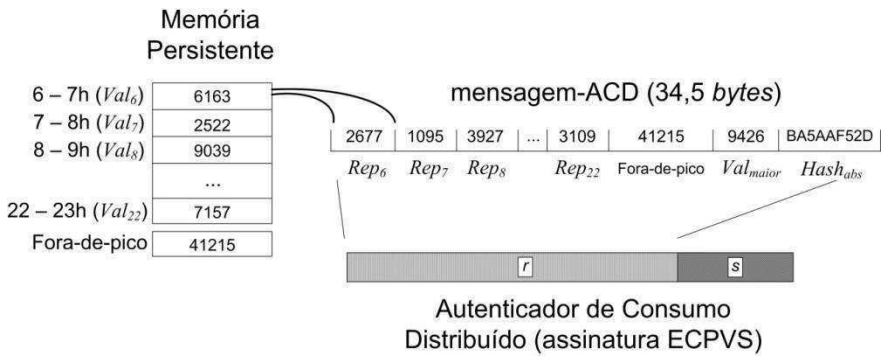

Figura 11. Exemplo de composição do ACD pela Técnica por Quantização Escalar (k_{esc} = 12 e h_{esc} = 36).

Dessa forma, além das 17 representações dos registradores referentes aos horários entre 6h-23h, será reservado um bloco de 20 bits para o valor absoluto consumido no horário fora-de-pico, 16 bits para o maior valor entre todos os registradores, Val_{maior},e um bloco para o valor $Hash_{abs.}$

O $Hash_{abs}$ é resultado de uma função de *hash* (SHA-224 ou equivalente/superior) dos valores absolutos dos 17 valores concatenados dos registradores e separados por vírgula ("Val_6 ,Val_7 ,Val_8 , ... , Val_{22}"). Do resultado dado pela função de *hash* escolhida, aproveitam-se os últimos h_{esc} bits. O $Hash_{abs}$ é de grande importância para o algoritmo de checagem durante o Processo de Verificação da Medição, uma vez que ele guarda uma rastreabilidade para os valores absolutos de cada registradores, ou seja, os dados originais guardados no módulo TMM.

Na Figura 11, apresentamos um exemplo de composição da mensagem-ACD para k_{esc} = 12 e h_{esc} = 36. Na seção de testes e resultados (seção 5.6), realizamos simulações para achar o k_{esc} e o h_{esc} mais apropriados para essa técnica.

O **algoritmo de descompressão**, durante o PVM, reconstrói o caminho inverso da composição da mensagem-ACD, ou seja, a partir dos dados na mensagem, ele recupera os valores absolutos dos registradores. Para isso, o algoritmo deverá operar com as seguintes etapas:

1. Computar lista $lValCand_i$ de todos os possíveis valores candidatos para Rep_i, i ϵ [6, 22];
2. Computar todas as combinações de elementos de ($lValCand_i$, ... , $lValCand_{i+j}$), o qual este grupo pertence a uma faixa de preço e a soma dos seus elementos é igual ao consumo da faixa de preço apresentado como entrada do algoritmo. Adicionar essas combinações em $lSeqCand_{posto}$ (Lista de Sequências Candidatas por Posto);
3. Incluir a combinação de todas as $lSeqCand_{posto}$ em lSeqComb;
4. Obter o valor de Hash() para todos os elementos de lSeqComb;
5. Quando houver igualdade com $Hash_{abs}$, os valores de consumo originais (Val_i) foram recuperados.

Com os dados originais recuperados, e *overhead* criptográfico verificado, isso significa que a validação da medição foi positiva e o PVM realizado com sucesso.

O Algoritmo 1 apresenta o algoritmo de descompressão responsável pela execução das etapas mostradas anteriormente.

Algoritmo 1: Algoritmo de descompressão (aplicável às técnicas das seções 5.3, 5.4 e 5.5)

```
# autenticador de consumo
var auth
# configuração dos postos tarifários (início e fim de cada posto)
var postos_config[]
# valores de consumo de cada posto tarifário
var postos_val[]
# hash_abs
var hash_abs
# lista de representações na mensagem
var rep[]
# lista de valores candidados de cada representação
var lValCand[]
# lista de valores de sequências candidatas por posto
var lSeqCand[]
# lista de valores de sequências candidatas combinadas
var lSeqComb[]
```

```
proc descomprimir_auth(var auth, var postos_config[], var postos_val[])
   do rep[], hash_abs := separa_dados_mensagem(auth)
      for each rep_i in rep[]
         lValCand[rep_i] := busca_candidatos_rep(rep_i)
      rof
      for each posto in postos_config
         lSeqCand[posto]:= busca_candidatos_seq(lValCand[], postos_val[posto])
      rof
      lSeqComb[] := combinar_todas_seq(lSeqCand[])
      for each seq in lSeqComb[]
         if Hash(seq) == hash_abs
            descompressao := true
      rof
   od
```

5.4 Técnica por Contadores em Módulo

A Técnica por Contadores em Módulo descreve outra forma de realizar a compressão lógica dos dados originados no módulo TMM. Essa técnica estabelece que o valor de consumo de um registrador horário i, Val_i, é representado por um contador sequencial crescente que é incrementado ao passo que Val_i também é incrementado, porém restringido a um intervalo de inteiros $[0, 2^{k_{mod}}-1]$, $k_{mod} < 16$, ou seja, o número absoluto de consumo Val_i será representado em módulo $2^{k_{mod}}$.

Então, para esta técnica, usaremos k_{mod} bits para a representação Rep_i dos valores Val_i. Logo, Rep_i será calculado pela Equação 3.

$$Rep_i = Val_i \mod 2^{k_{mod}}$$

Equação 3. Cálculo da representação Rep_i pela Técnica por Contadores em Módulo.

A mensagem-ACD pela Técnica por Contadores em Módulo é composta pelos seguintes dados:

a. Soma dos horários fora-de-pico (23h-5:59h, finais-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): $(17 \times k_{mod})$ bits;

c. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): h_{mod} bits.

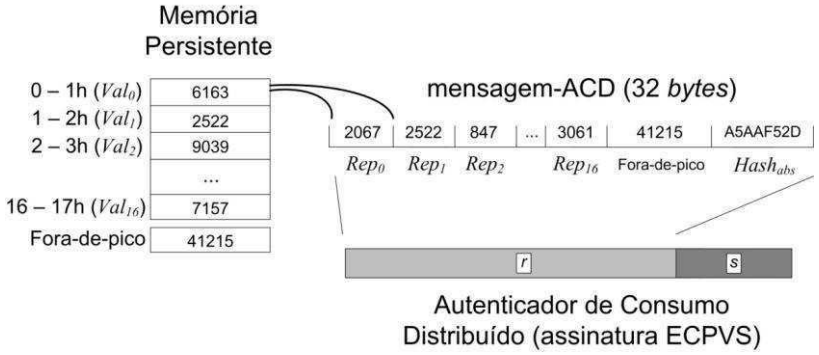

Figura 12. Exemplo de composição do ACD pela Técnica por Contadores em Módulo (k_{mod} = 12 e h_{mod} = 32).

De uma forma geral, a composição é bem parecida com a Técnica por Quantização Escalar apenas com a exceção do dado de maior valor entre todos os registradores, Val_{maior}.

O algoritmo de descompressão do Processo de Verificação da Medição também é realizado de forma semelhante à técnica anterior, incluindo a escolha dos valores candidatos, busca pelas sequências candidatas, formando *lSeqCand*, e comparação do *hash* das sequências candidatas de *lSeqComb* até encontrar uma correspondente ao $Hash_{abs}$.

5.5 Técnica por Contadores em Função de Dispersão

A Técnica por Contadores em Função de Dispersão apresenta uma estrutura idêntica a Técnica de Contadores em Módulo. Sua diferença (e grande vantagem, como veremos nos testes realizados na seção 5.6) está no fato de que o valor de consumo de um registrador *i* de hora, Val_i, será representado por uma sequência aleatória, e não mais por um contador sequencial, como na técnica anterior. Os valores desse contador aleatório também estão restringidos por um intervalo de inteiros $[0, 2^{k_{hash}}-1]$, sendo $k_{hash} < 16$.

Usando-se k_{hash} bits para a representação Rep_i do valor do registrador *i*, Val_i. O valor de Rep_i será calculado através da Equação 4.

$$Rep_i = UltimosBits(k_{hash}, Hash(\ concat(\ Val_i\ , ID_i)\ ))$$

Equação 4. Cálculo da representação Rep_i pela Técnica por Contadores em Função de Dispersão.

A função *Hash()* representa qualquer função com propriedade unidirecional, com resistência a colisões e que gere um dado de saída com pelo menos k_{hash} bits. Para essa técnica, convencionou-se utilizar os últimos k_{hash} bits da saída da função *Hash()* para

preencher Rep_i, porém outra combinação qualquer de bits resultantes poderia ter sido escolhida .

A concatenação de Val_i com um identificador próprio da faixa é justificado por uma questão de melhoria na segurança do autenticador. Com o identificador por faixa, o resultado da função *Hash()* para um mesmo valor de consumo terão representações diferentes dependendo do registrador em que o valor estiver localizado. Essa manobra atribui aos Rep_i uma aleatoriedade entre si, dificultando ainda mais um possível ataque de injeção de dados falsos.

A composição da mensagem-ACD pela Técnica por Contadores em Função de Dispersão contém os seguintes dados abaixo (igual à técnica por módulo):

a. Soma dos horários fora-de-pico (23h-5:59h, finais-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): ($17 \times k_{hash}$) bits;

c. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): h_{hash} bits.

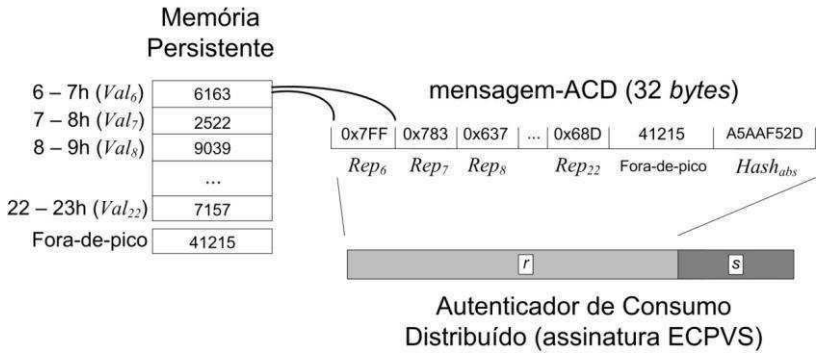

Figura 13. Exemplo de composição do ACD pela Técnica por Contadores em Função de Dispersão (k_{hash} = 12 e h_{hash} = 32).

O algoritmo de descompressão faz uso de Tabelas *Rainbow* durante o procedimento de listagem de valores candidatos para $lValCand_i$. Essas tabelas mapeiam os valores de *hash* para seus respectivos valores *concat*(Val_i, ID_i), onde $Val_i \in [0, 40.000]$ e $i \in [0, 16]$. O algoritmo de descompressão, então, inicia da seguinte maneira: (**i**) procura por todos os *hashes* que possuem os últimos k_{hash} bits igual a Rep_i; e (**ii**) inclui os respectivos valores desses *hashes* em $lValCand_i$. O restante do algoritmo segue da forma descrita na seção 5.3.

5.6 Análise Experimental das Técnicas e Resultados

Nesta seção, apresentamos os testes realizados com as técnicas de compressão descritas anteriormente e resolvemos o valor de *k* e *h* apropriado para cada uma.

De fato, essas técnicas utilizam algoritmos de compressão **assimétricos**, uma vez que o tempo gasto para recuperar os dados comprimidos pode ser bem maior do que o tempo de compressão, isso dependendo do valor usado em k_{esc}, k_{mod}, k_{hash}. Outro conceito importante é a **diferença entre os valores maior e menor dos registradores em cada posto tarifário** ($Interval_{max} = Val_{max} - Val_{min}$). Espera-se que $\boldsymbol{Interval_{max}}$ não ultrapasse o valor de 10.000 kWh, uma vez que o consumo de uma unidade consumidora operando sob uma modalidade tarifária horo-sazonal tende a ser mais equilibrada durante o dia. Conforme $Interval_{max}$ aumenta com o passar dos anos, e devido a uma etapa de força-bruta nos algoritmos de descompressão, este processo de descompressão pode tomar bastante tempo. O tempo máximo assumido para descompressão é de até 60 segundos, como esperado nos requisitos do projeto.

Primeiramente, iremos determinar *k*, o número apropriado de bits para Rep_i, para cada técnica e encontrar o melhor *trade-off* entre o tempo de descompressão e o tamanho total da mensagem-ACD. Para isso, **formulamos 140 cenários variando *k* e $\boldsymbol{Interval_{max}}$ para cada técnica em uma modalidade tarifária existente** e analisamos o tempo necessário de execução do algoritmo de descompressão do mensagem-ACD. O experimento foi realizado detalhadamente como segue. Para cada k_{esc}, k_{mod}, $k_{hash} \in [8, 14]$ e para cada $Interval_{max}$ múltiplo de 1.000 pertencente ao intervalo [1.000, 20.000], foram simulados 100 ACDs em duas modalidades tarifárias reais existentes: (**i**) a do Ontario Energy Board e (**ii**) a Tarifa Branca da ANEEL. A simulação foi realizada em um PC, Intel Q6600 CPU 2.40GHz, 8GB RAM. Os autenticadores ACD simulados e as técnicas de compressão/descompressão de dados foram implementados em linguagem C++. Para o cálculo das Tabelas *Rainbow*, de $Hash_{abs}$ e implementação de *Hash()*, foi utilizado a função SHA-224.

Na segunda parte dos experimentos, determinaremos *h*, o número mínimo de bits para $Hash_{abs}$, para cada técnica e encontrar o melhor *trade-off* entre a probabilidade de se obter uma resposta não-única do algoritmo de descompressão e o tamanho de $Hash_{abs}$. Para isso, **simulamos um conjunto de 1.000 ACDs** para cada técnica e **fixamos a probabilidade *p* de uma solução não-única deveria ser $p < 0{,}01$**. Esse estudo é apresentado na seção 5.6.2.

5.6.1 Determinando *k*

Para cada técnica e para cada modalidade tarifária existe uma tabela com resultados do tempo de descompressão médio de um autenticador ACD. O tempo de descompressão corresponde a todo tempo gasto pelo algoritmo de descompressão incluindo uma **busca completa**, o que significa que o algoritmo não finaliza ao achar a primeira solução, e sim continua até testar todas as possibilidades de solução. Isso garante ao verificador que uma mensagem-ACD está relacionada somente a um conjunto de valores Val_i. Os valores comentados durante essa análise estão destacados em negrito nas tabelas. Os valores representados por "-" foram descartados por serem inviáveis de serem computados em tempo hábil, no entanto não interferem na conclusão dos resultados obtidos.

Primeiramente, analisaremos a Técnica por Quantização Escalar. Para os testes realizados com a modalidade tarifária do OEB, da Tabela 1 concluímos a inviabilidade de descompressão para $k_{esc} < 9$ e definimos $\boldsymbol{k_{esc} = 12}$ como sendo a opção de melhor custo-benefício por suportar um $\boldsymbol{Interval_{max}}$ **= 11.000 kWh** e um tempo de descompressão médio (μ) = **39,4 segundos** com intervalo de confiança [23,3 ≤ μ ≤ 55,4] (μ ± 40,73%) ao nível de confiança = **95%**. Da Tabela 2, com os testes realizados com a modalidade Tarifa Branca, concluímos também que $\boldsymbol{k_{esc} = 12}$, permitindo um $\boldsymbol{Interval_{max}}$ **= 10.000 kWh** e um tempo de descompressão médio (μ) = **17,9 segundos** com intervalo de confiança [12,1 ≤ μ ≤ 23,6] (μ ± 32,12%) ao nível de confiança = **95%**.

Tabela 1. Tempo de descompressão x $Interval_{max}$, k_{esc} ϵ [8, 14], modalidade Ontario Energy Board – Técnica por Quantização Escalar.

$Interval_{max}$ (kWh)	Tempo para descompressão (seg)						
	k_{esc} = 8	k_{esc} = 9	k_{esc} = 10	k_{esc} = 11	k_{esc} = 12	k_{esc} = 13	k_{esc} = 14
1000	-	8,31E-01	2,92E-03	2,87E-03	2,78E-03	2,91E-03	2,82E-03
2000	-	2,08E+03	7,54E-01	2,37E-03	2,34E-03	2,45E-03	2,33E-03
3000	-	-	6,84E+01	1,08E-01	2,40E-03	2,47E-03	2,36E-03
4000	-	-	2,01E+03	9,83E-01	2,26E-03	2,44E-03	2,36E-03
5000	-	-	-	1,98E+01	9,83E-03	2,32E-03	2,41E-03
6000	-	-	-	9,62E+01	9,05E-02	2,35E-03	2,19E-03
7000	-	-	-	8,02E+02	5,31E-01	2,38E-03	1,35E-03
8000	-	-	-	-	7,91E-01	2,34E-03	1,40E-03
9000	-	-	-	-	4,51E+00	3,59E-03	1,25E-03
10000	-	-	-	-	1,43E+01	1,21E-02	1,32E-03
11000	-	-	-	-	**3,94E+01**	4,77E-02	1,37E-03
12000	-	-	-	-	8,84E+01	1,25E-01	1,36E-03
13000	-	-	-	-	4,59E+02	2,04E-01	1,30E-03
14000	-	-	-	-	-	2,66E-01	1,35E-03
15000	-	-	-	-	-	5,79E-01	1,42E-03
16000	-	-	-	-	-	6,44E-01	1,36E-03
17000	-	-	-	-	-	1,59E+00	1,53E-03
18000	-	-	-	-	-	3,97E+00	3,32E-03
19000	-	-	-	-	-	8,57E+00	5,82E-03
20000	-	-	-	-	-	1,31E+01	1,09E-02

Tabela 2. Tempo de descompressão x Interval$_{max}$, k$_{esc}$ ϵ [8, 14], modalidade Tarifa Branca – Técnica por Quantização Escalar.

Interval$_{max}$ (kWh)	Tempo para descompressão (seg)						
	k$_{esc}$ = 8	k$_{esc}$ = 9	k$_{esc}$ = 10	k$_{esc}$ = 11	k$_{esc}$ = 12	k$_{esc}$ = 13	k$_{esc}$ = 14
1000	-	1,18E+00	3,15E-03	3,01E-03	2,96E-03	3,08E-03	3,04E-03
2000	-	3,20E+03	1,27E+00	2,40E-03	2,47E-03	2,46E-03	2,41E-03
3000	-	-	1,35E+02	1,18E-01	2,42E-03	2,43E-03	2,55E-03
4000	-	-	-	1,30E+00	2,48E-03	2,51E-03	2,65E-03
5000	-	-	-	2,11E+01	1,42E-02	2,30E-03	2,67E-03
6000	-	-	-	1,48E+02	1,79E-01	2,31E-03	2,36E-03
7000	-	-	-	7,24E+02	3,95E-01	2,48E-03	2,48E-03
8000	-	-	-	-	1,87E+00	2,08E-03	2,54E-03
9000	-	-	-	-	5,10E+00	4,27E-03	2,70E-03
10000	-	-	-	-	**1,79E+01**	1,32E-02	2,67E-03
11000	-	-	-	-	5,76E+01	6,98E-02	2,79E-03
12000	-	-	-	-	3,83E+02	1,21E-01	2,36E-03
13000	-	-	-	-	3,51E+02	2,56E-01	2,28E-03
14000	-	-	-	-	7,41E+02	6,22E-01	2,57E-03
15000	-	-	-	-	-	7,88E-01	2,46E-03
16000	-	-	-	-	-	1,44E+00	2,46E-03
17000	-	-	-	-	-	2,86E+00	2,54E-03
18000	-	-	-	-	-	4,41E+00	3,62E-03
19000	-	-	-	-	-	1,14E+01	9,40E-03
20000	-	-	-	-	-	2,30E+01	1,95E-02

A Tabela 3 apresenta os resultados da simulação obtidos com a Técnica de Contadores em Módulo para a modalidade tarifária da OEB. Dessa tabela, devemos considerar, para o tempo de descompressão abaixo de um minuto, k_{mod} = 11 permitindo um $Interval_{max}$ = 6.000 kWh e k_{mod} = 12 permitindo um $Interval_{max}$ = 13.000 kWh. Apesar de a primeira opção oferecer um tamanho menor para a mensagem-ACD, seu $Interval_{max}$ permitido é pequeno para garantir um tempo de descompressão aceitável durante a vida útil do medidor. Logo, definiremos $\boldsymbol{k_{mod}}$ **= 12** como a opção de melhor custo-benefício, com um tempo de descompressão médio (μ) = **46,1 segundos** e intervalo de confiança [28,2 ≤ μ ≤ 63,9] (μ ± 38,68%) ao nível de confiança = **95%**. Da Tabela 4, tiramos uma conclusão semelhante, onde k_{mod} = 12 é o mais apropriado, permitindo um $\boldsymbol{Interval_{max}}$ **= 13.000 kWh** e um tempo de descompressão médio (μ) = **22,9 segundos** com intervalo de confiança [14,3 ≤ μ ≤ 31,4] (μ ± 37,34%) ao nível de confiança = **95%**.

Tabela 3. Tempo de descompressão x $Interval_{max}$, k_{mod} ϵ [8, 14], modalidade Ontario Energy Board – Técnica por Contadores em Módulo.

$Interval_{max}$ (kWh)	Tempo para descompressão (seg)						
	k_{mod} = 8	k_{mod} = 9	k_{mod} = 10	k_{mod} = 11	k_{mod} = 12	k_{mod} = 13	k_{mod} = 14
1000	8,87E+02	7,56E-02	5,64E-05	5,64E-05	5,64E-05	5,64E-05	5,64E-05
2000	1,36E+07	9,51E+02	7,75E-02	5,64E-05	5,64E-05	5,64E-05	5,64E-05
3000	1,75E+09	2,54E+05	1,64E+01	4,00E-03	5,64E-05	5,64E-05	5,64E-05
4000	-	1,42E+07	7,73E+02	8,48E-02	5,64E-05	5,64E-05	5,64E-05
5000	-	1,03E+08	1,62E+04	2,07E+00	3,51E-04	5,64E-05	5,64E-05
6000	-	-	2,24E+05	**1,93E+01**	4,05E-03	5,64E-05	5,64E-05
7000	-	-	2,06E+06	1,49E+02	2,06E-02	5,64E-05	5,64E-05
8000	-	-	1,33E+07	9,07E+02	8,04E-02	5,64E-05	5,64E-05
9000	-	-	4,34E+07	4,67E+03	4,58E-01	9,71E-05	5,64E-05
10000	-	-	1,97E+07	1,74E+04	2,15E+00	3,25E-04	5,64E-05
11000	-	-	-	7,19E+04	5,82E+00	1,32E-03	5,64E-05
12000	-	-	-	2,29E+05	1,45E+01	4,78E-03	5,64E-05
13000	-	-	-	7,87E+05	**4,61E+01**	1,16E-02	5,64E-05
14000	-	-	-	1,83E+06	1,52E+02	2,64E-02	5,64E-05
15000	-	-	-	5,62E+06	3,76E+02	4,45E-02	5,64E-05
16000	-	-	-	1,34E+07	8,03E+02	7,14E-02	5,64E-05
17000	-	-	-	2,90E+07	2,20E+03	1,25E-01	5,93E-05
18000	-	-	-	-	4,49E+03	4,70E-01	1,06E-04
19000	-	-	-	-	1,05E+04	8,34E-01	1,76E-04
20000	-	-	-	-	1,79E+04	2,01E+00	2,89E-04

Tabela 4. Tempo de descompressão x $Interval_{max}$, k_{mod} ϵ [8, 14], modalidade Tarifa Branca – Técnica por Contadores em Módulo.

$Interval_{max}$ (kWh)	Tempo para descompressão (seg)						
	k_{mod} = 8	k_{mod} = 9	k_{mod} = 10	k_{mod} = 11	k_{mod} = 12	k_{mod} = 13	k_{mod} = 14
1000	3,18E+02	3,11E-02	2,82E-03	2,88E-03	3,10E-03	2,70E-03	2,70E-03
2000	-	4,28E+02	3,12E-02	2,37E-03	2,29E-03	2,28E-03	2,17E-03
3000	-	-	7,15E+00	4,50E-03	2,32E-03	2,50E-03	2,24E-03
4000	-	-	6,48E+02	3,23E-02	2,29E-03	2,40E-03	2,24E-03
5000	-	-	-	6,65E-01	2,46E-03	2,21E-03	2,27E-03
6000	-	-	-	**6,13E+00**	4,38E-03	2,31E-03	2,56E-03
7000	-	-	-	6,64E+01	1,24E-02	2,31E-03	2,26E-03
8000	-	-	-	3,42E+02	3,08E-02	2,29E-03	2,24E-03
9000	-	-	-	-	1,96E-01	2,39E-03	2,21E-03
10000	-	-	-	-	8,07E-01	2,52E-03	2,24E-03
11000	-	-	-	-	2,43E+00	3,00E-03	2,38E-03
12000	-	-	-	-	6,54E+00	4,85E-03	2,35E-03
13000	-	-	-	-	**2,29E+01**	6,58E-03	2,26E-03
14000	-	-	-	-	6,14E+01	1,13E-02	2,32E-03
15000	-	-	-	-	1,56E+02	1,88E-02	2,35E-03
16000	-	-	-	-	4,90E+02	3,54E-02	2,23E-03
17000	-	-	-	-	8,76E+02	8,10E-02	2,24E-03
18000	-	-	-	-	-	1,94E-01	2,33E-03
19000	-	-	-	-	-	4,00E-01	2,35E-03
20000	-	-	-	-	-	7,82E-01	2,56E-03

A Tabela 5 apresenta os dados simulados referentes à Técnica de Contadores em Função de Dispersão pela modalidade tarifária da OEB. Dessa tabela, constatamos que para k_{hash} = 10, com um $\boldsymbol{Interval_{max}}$ **= 13.000 kWh**, alcançamos um tempo de descompressão médio (μ) = **38,4 segundos** com intervalo de confiança [24,8 ≤ μ ≤ 51,9] (μ ± 35,41%) ao nível de confiança = **95%**. No entanto, a Tabela 6, que representa os dados simulados na modalidade Tarifa Branca, indica que a escolha mais apropriada é k_{hash} = 11, permitindo um

***Interval*$_{max}$ = 11.000** kWh e um tempo de descompressão médio (μ) = **43,0 segundos** com intervalo de confiança [27,4 ≤ μ ≤ 58,5] (μ ± 36,17%) ao nível de confiança = **95%**. Para determinar o k_{hash}, escolheremos a opção menos restritiva a fim de viabilizar as duas modalidades tarifárias. Logo, para a Técnica de Contadores em Função de Dispersão, definiremos ***k*$_{hash}$ = 11** como a opção mais apropriada.

Tabela 5. Tempo de descompressão x Interval$_{max}$, k$_{hash}$ ϵ [8, 14], modalidade Ontario Energy Board – Técnica por Contadores em Função de Dispersão.

Interval$_{max}$ (kWh)	Tempo para descompressão (seg)						
	k$_{hash}$ = 8	k$_{hash}$ = 9	k$_{hash}$ = 10	k$_{hash}$ = 11	k$_{hash}$ = 12	k$_{hash}$ = 13	k$_{hash}$ = 14
1000	1,37E-02	3,28E-03	3,40E-03	3,25E-03	3,21E-03	3,17E-03	3,30E-03
2000	8,06E+00	5,14E-03	2,92E-03	2,75E-03	2,79E-03	2,84E-03	2,80E-03
3000	7,88E+02	7,15E-02	2,98E-03	2,69E-03	2,61E-03	2,73E-03	2,99E-03
4000	2,66E+04	8,97E-01	3,90E-03	2,77E-03	2,72E-03	2,91E-03	2,65E-03
5000	6,46E+05	1,03E+01	6,29E-03	2,80E-03	2,73E-03	2,84E-03	2,79E-03
6000	1,15E+07	9,79E+01	1,51E-02	2,95E-03	2,61E-03	2,88E-03	3,30E-03
7000	-	1,10E+03	6,03E-02	3,08E-03	2,94E-03	2,83E-03	2,69E-03
8000	-	6,81E+03	1,67E-01	3,55E-03	2,80E-03	2,74E-03	2,77E-03
9000	-	1,99E+04	8,03E-01	3,86E-03	2,88E-03	2,80E-03	2,81E-03
10000	-	8,02E+04	1,67E+00	5,09E-03	2,85E-03	2,65E-03	2,66E-03
11000	-	3,33E+05	6,81E+00	5,48E-03	2,75E-03	2,76E-03	2,87E-03
12000	-	-	1,84E+01	7,88E-03	3,00E-03	2,92E-03	3,15E-03
13000	-	-	**3,84E+01**	1,12E-02	2,85E-03	2,84E-03	2,84E-03
14000	-	-	9,31E+01	2,03E-02	3,03E-03	2,92E-03	3,11E-03
15000	-	-	2,35E+02	2,19E-02	3,05E-03	2,84E-03	2,88E-03
16000	-	-	4,71E+02	4,42E-02	3,27E-03	2,90E-03	2,88E-03
17000	-	-	1,19E+03	6,29E-02	3,34E-03	2,99E-03	2,80E-03
18000	-	-	1,97E+03	1,14E-01	3,50E-03	2,92E-03	2,96E-03
19000	-	-	5,83E+03	2,03E-01	3,49E-03	2,80E-03	2,68E-03
20000	-	-	1,03E+04	3,33E-01	4,13E-03	2,94E-03	3,31E-03

Tabela 6. Tempo de descompressão x Interval$_{max}$, k$_{hash}$ ϵ [8, 14], modalidade Tarifa Branca – Técnica por Contadores em Função de Dispersão.

Interval$_{max}$ (kWh)	Tempo para descompressão (seg)						
	k$_{hash}$ = 8	k$_{hash}$ = 9	k$_{hash}$ = 10	k$_{hash}$ = 11	k$_{hash}$ = 12	k$_{hash}$ = 13	k$_{hash}$ = 14
1000	3,73E+00	2,27E-02	3,56E-03	3,21E-03	3,20E-03	3,20E-03	3,15E-03
2000	-	2,74E+00	1,38E-02	3,01E-03	2,87E-03	2,61E-03	2,73E-03
3000	-	9,72E+01	2,69E-01	4,75E-03	2,90E-03	2,61E-03	2,70E-03
4000	-	-	2,83E+00	1,30E-02	2,89E-03	2,59E-03	3,21E-03
5000	-	-	3,08E+01	8,84E-02	3,10E-03	2,78E-03	2,67E-03
6000	-	-	2,11E+02	3,25E-01	4,44E-03	2,74E-03	2,67E-03
7000	-	-	-	1,01E+00	9,29E-03	2,81E-03	2,66E-03
8000	-	-	-	2,95E+00	1,29E-02	2,90E-03	2,69E-03
9000	-	-	-	8,28E+00	2,41E-02	3,07E-03	2,74E-03
10000	-	-	-	2,24E+01	6,23E-02	3,22E-03	2,74E-03
11000	-	-	-	**4,30E+01**	1,03E-01	3,37E-03	2,70E-03
12000	-	-	-	1,59E+03	3,20E-01	4,19E-03	2,72E-03
13000	-	-	-	-	3,89E-01	4,82E-03	2,75E-03
14000	-	-	-	-	7,59E-01	6,45E-03	2,84E-03
15000	-	-	-	-	2,13E+00	7,91E-03	2,83E-03
16000	-	-	-	-	1,97E+00	9,43E-03	2,85E-03
17000	-	-	-	-	5,09E+00	1,70E-02	2,81E-03
18000	-	-	-	-	1,17E+01	3,76E-02	2,96E-03
19000	-	-	-	-	1,41E+01	3,24E-02	3,24E-03
20000	-	-	-	-	2,97E+01	4,82E-02	3,12E-03

A modalidade Tarifa Branca tende sempre a ser mais restritiva do que a modalidade do OEB, pois ela tem uma configuração horária que reserva um período relativamente grande

para o posto tarifário fora-de-pico, 19 horas, contra 12 horas da modalidade do OEB. Para o algoritmo de descompressão, esse fator **aumenta significativamente o número de sequências candidatas** que ele precisa testar (fazemos uma busca sequencial) e, por isso, o aumento no tempo final da solução. Dois melhoramentos futuros considerados são: aplicar um algoritmo de busca otimizado, com uma boa heurística, e usar paralelismo na programação, no entanto, essas abordagens não estão no escopo deste trabalho.

Em resumo, através das simulações realizadas, pudemos fixar os valores de bits para as representações Rep_i de cada técnica. Para a Técnica por Quantização Escalar, $k_{esc} = 12$, para a Técnica por Contadores em Módulo, $k_{mod} = 12$ e, para a Técnica por Contadores em Função de Dispersão, $k_{esc} = 11$.

5.6.2 Determinando *h*

Durante a penúltima etapa do algoritmo de descompressão, algumas sequências candidatas para representação dos valores originais, Val_i, dos registradores do módulo TMM são consideradas. Para encontrar qual sequência é a correta, a mensagem-ACD contém uma informação importante: $\boldsymbol{Hash_{abs}}$, um *hash* computado dos valores originais. Para cada técnica, iremos calcular o número de bits mínimo, *h*, para essa informação.

Para cada técnica, com seu *k* devidamente ajustado e no máximo de seu $Interval_{max}$ permitido, simulamos um total de 1.000 autenticadores ACD na modalidade Tarifa Branca e realizamos o processo de descompressão. Para cada autenticador, anotamos quantas sequências candidatas foram achadas e destacamos o autenticador que teve o maior número de sequências a serem comparadas com $Hash_{abs.}$ A partir do maior número de sequências candidatas obtido para um autenticador e a partir da probabilidade de achar uma solução não-única *p* ($p < 0,01$), concluímos *h*. O resultado da simulação do número de sequências candidatas por autenticador ACD pode ser visto na Figura 14, Figura 15 e Figura 16.

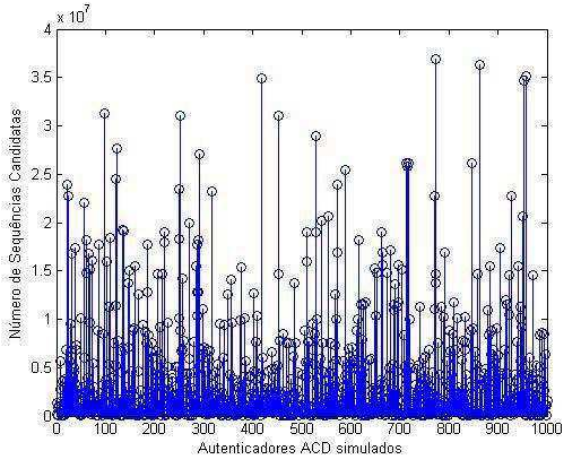

Figura 14. Número de Sequências Candidatas em 1000 autenticadores ACD simulados pela Técnica por Quantização Escalar.

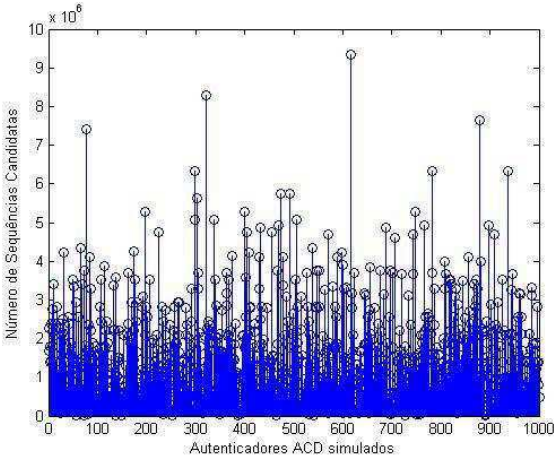

Figura 15. Número de Sequências Candidatas em 1000 autenticadores ACD simulados pela Técnica por Contadores em Módulo.

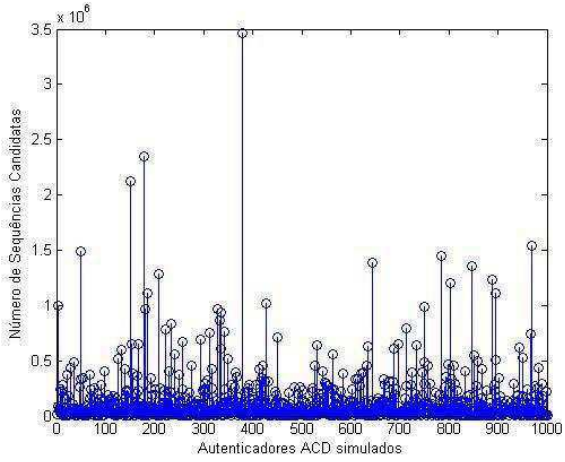

Figura 16. Número de Sequências Candidatas em 1000 autenticadores ACD simulados pela Técnica por Contadores em Função de Dispersão.

A Tabela 7 mostra o resumo da simulação, indicando o maior número, $Maior_{nseq}$, e o número médio de sequências candidatas obtidos para cada técnica, além dos h_s mínimos para a probabilidade p determinada. O cálculo de h é determinado pela Equação 5.

$$\frac{Maior_{nseq}}{2^h} < 0{,}01$$

Equação 5. Cálculo de *h* em função do maior Número de Sequências candidatas obtidas na simulação.

Em resumo, obtemos $h_{esc} = 32$, $h_{mod} = 30$ e $h_{hash} = 29$ como número mínimo de bits para $Hash_{abs}$. Embora este seja o mínimo requerido, poderemos eventualmente usar mais bits para representar $Hash_{abs}$ para fins de arredondamento do tamanho total da mensagem-ACD, como veremos na seção seguinte.

Tabela 7. Resumo da simulação para determinação de *h* mínimo para cada técnica.

Técnica	Número de Seq. Candidatas		*h* (p < 0,01)
	Médio	Maior	
Quantização	4.120.447	36.880.704	32
Módulo	1.495.288	9.353.589	30
Fç. Dispersão	124.219	3.461.389	29

5.6.3 Resultados

Nesta seção, concluímos o tamanho final dos autenticadores ACD compostos por cada técnica de compressão de dados e os comparamos ao final.

Pela Técnica por Quantização Escalar, o tamanho final do autenticador ACD (r, s) é de 34,25 + 28 = **62,25 bytes**, resultando em **83 caracteres** codificados em base64. O tamanho de $Hash_{abs}$ foi aumentado para 34 bits por questões de arredondamento da codificação base64, a fim de se evitar o *padding* da codificação. Os dados que compõe a mensagem-ACD e seus devidos tamanhos seguem abaixo:

a. Soma dos períodos fora-de-pico (Val_{23} - Val_5, fins-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): (17 × 12) = 204 bits;

c. O maior valor absoluto entre todos os registradores (Val_{maior}): 16 bits;

d. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): 34 bits.

Em seguida, para a Técnica de Contadores em Módulo, o tamanho final do autenticador ACD (*r*, *s*) é de 32 + 28 = **60 bytes**, resultando em **80 caracteres** codificados em base64. O tamanho de $Hash_{abs}$ também foi aumentado por questões de arredondamento da codificação usada. Finalmente, a mensagem-ACD é formada com os seguintes dados:

a. Soma dos horários fora-de-pico (23h-5:59h, finais-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): (17 × 12) = 204 bits;

c. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): 32 bits.

Finalmente, para a Técnica de Contadores em Função de Dispersão, o tamanho do autenticador ACD (*r*, *s*) ficou em 29,75 + 28 = **57,75 bytes**, resultando em **77 caracteres** codificados em base64. O tamanho de $Hash_{abs}$ também foi aumentado em 2 bits por questões de arredondamento da codificação base64. Finalmente, a mensagem-ACD é formada pelos seguintes dados:

a. Soma dos horários fora-de-pico (23h-5:59h, finais-de-semana e feriados): 20 bits;

b. As 17 representações dos registradores restantes (Rep_6 - Rep_{22}): (17 × 11) = 187 bits;

c. *Hash* dos 17 valores (Val_6 - Val_{22}) de cada registrador concatenados ($Hash_{abs}$): 31 bits.

Pela Técnica de Contadores em Função de Dispersão, conseguimos diminuir o tamanho da mensagem-ACD para **238 bits**, contra **256 bits** da Técnica de Contadores em Módulo, **274 bits** da Técnica por Quantização Escalar e 322 bits da mensagem-ACD usada na Técnica de Valores Absolutos.

A redução em mais de 1/4 do tamanho da mensagem-ACD foi conseguida por técnicas apresentadas neste trabalho. Algoritmos mais comuns usados para compressão de dados, como os baseados em dicionário, não teriam o mesmo sucesso ao processarem uma

mensagem de tamanho pequeno como entrada. Em geral, esses algoritmos necessitam de, no mínimo, 1.000 bytes de dados de entrada para tornarem-se eficientes (CHU 1996).

O autenticador ACD, como um todo, teve uma redução de **30%** no tamanho desde sua primeira tentativa de composição, caindo de 110 para 77 caracteres, tornando-se mais prático para transcrição.

5.7 Abordagens Alternativas de Autenticador

Nesta seção, analisaremos abordagens alternativas ao Autenticador de Consumo Distribuído por Hora. Embora essas alternativas apresentem vantagens em alguns pontos em relação ao autenticador ACD, elas falham em atender o conjunto total de requisitos especificados para este projeto. Contudo, são alternativas viáveis e que possuem relevância como solução do nosso problema como um todo.

5.7.1 Autenticador Relativo

O Autenticador Relativo parte do conceito que o usuário pode verificar as medições realizadas pelo medidor inteligente em um **período compreendido entre a "coleta" de dois autenticadores de consumo** juntamente com os valores de consumo totalizados em cada faixa de preço. Dessa forma, o usuário poderia realizar, como exemplo, uma coleta em um momento t_1 e a segunda coleta em um momento t_2, e atestar a validade das operações do medidor durante este período.

O período máximo que iremos considerar para realizar uma verificação da medição será de 48 horas, dessa forma espera-se sempre uma diferença pequena entre os valores de consumo coletados em t_1 e t_2. Por convenção, o autenticador relativo irá zerar seus dados às 00h de cada dia ímpar do mês para, assim, iniciar uma nova janela de verificação. A verificação dos dados de medição é realizada comparando-se a diferença de consumo entre os dados coletados do visor do medidor e a diferença dos dados contidos nos autenticadores. Caso a diferença seja a mesma, a medição estará validada.

Para compor esse autenticador utilizaremos o esquema de assinatura ECPVS, assim como os mesmos parâmetros de domínio usados para o autenticador ACD. A mensagem embutida no autenticador também deve ter os valores de consumo discriminados por hora, devido ao desconhecimento pelo módulo TMM da modalidade tarifária vigente. Contudo,

nenhuma transformação de dados é realizada para comprimir esses valores, isso porque a extensão do conjunto dos possíveis valores de consumo que precisam ser incluídos à mensagem do Autenticador Relativo é significativamente menor em relação ao conjunto de valores usados no autenticador ACD. A composição dos dados da mensagem do Autenticador Relativo segue abaixo:

a. Soma dos horários fora-de-pico (23h-5:59h, finais-de-semana e feriados): 8 bits;
b. As 17 valores horários de consumo (referentes à 00h do último dia ímpar): 4 bits para cada valor.

Com essa disposição de dados o tamanho final do autenticador (r, s) é de 9,5 + 28 = **37,5 bytes**, resultando em **50 caracteres** codificados em base64, **35% menor** do que um autenticador ACD usando a Técnica por Contadores em Função de Dispersão.

Embora exista a vantagem de obter um autenticador de consumo bem menor e sem a necessidade de realizar transformações de dados, o Autenticador Relativo apresenta algumas desvantagens como segue. Ele apenas garante **pequenas janelas de tempo de medição**, ao contrário do autenticador ACD que garante **todas as medições realizadas pelo medidor desde sua instalação**. Isso abre espaço para o medidor cometer pequenas fraudes entre as janelas de verificação. Outra questão é o fato de que é necessária a coleta de mais informações com a abordagem relativa, apesar de o autenticador ser menor, a coleta precisa ser realizada duas vezes. Por fim, a abordagem relativa não valida os valores do visor do medidor inteligente e também não poderia ser usada para validar o consumo impresso na conta de luz do usuário.

5.7.2 Autenticador de Consumo por Postos Tarifários

O Autenticador de Consumo por Postos Tarifários consiste em um conceito diferente do autenticador ACD. Nessa abordagem há o conhecimento por parte do módulo TMM da configuração da modalidade multitarifária sob a qual o medidor inteligente opera. Dessa forma, o módulo TMM poderá compor a mensagem a ser assinada totalizando o consumo pelas faixas de preço diferenciado.

Para que isso aconteça, o projeto do módulo TMM necessita ser alterado para permitir uma comunicação de dados segura entre este e a aplicação do fabricante do medidor. Dessa forma, a aplicação do medidor sempre informaria a configuração horária do próximo dia ao

módulo TMM. Por sua vez, o TMM acumularia o consumo de energia normalmente em cada registrador de hora e montaria a mensagem do autenticador de acordo com o que lhe foi informado pela aplicação do fabricante.

Diferentemente do autenticador ACD, o Autenticador de Consumo por Postos Tarifários **não possui uma mensagem embutida**, ou seja, a assinatura ECPVS só conterá o *overhead* criptográfico *s*. Isso se deve ao fato que esta mensagem é bem estruturada e pode ser montada também pelo algoritmo de verificação, não precisando ser informada embutida no autenticador. Os dados que a mensagem a ser assinada deve ter seguem abaixo:

a. Configuração da modalidade tarifária (hora início e hora fim de cada faixa de preço);

b. Valores acumulados e totalizados por postos tarifários.

Um exemplo dessa mensagem a sob a modalidade Tarifa Branca seria: "Posto1(18,19,20)=20000;Posto2(17,21)=9000;Posto3(0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,22,23,fds,fe)=40000".

Note que para a Tarifa Branca obtemos três postos tarifários (pico, intermediário e fora-de-pico), sendo os postos 1, 2 e 3 respectivamente. No posto 3, incluímos o valor de energia consumida também durante os finais-de-semana e feriados, por também serem contados como consumo fora-de-pico. Essa mensagem pode ser extensível a quantos postos a modalidade tarifária tiver.

Como o algoritmo de verificação conhece a modalidade tarifária informada e recebe de entrada os valores para cada posto, ele sabe remontar a mensagem assinada, o que torna desnecessária a inclusão da mensagem embutida no autenticador. Sendo assim, o tamanho do autenticador está diretamente relacionado ao tamanho da chave ECC usada para assinar a mensagem. Como estamos considerando os mesmos parâmetros de domínio usados no autenticador ACD, o tamanho total do Autenticador de Consumo por Postos Tarifários é de **28 bytes**, resultando em **40 caracteres** utilizando a codificação base64.

Embora essa abordagem se apresente como uma boa solução para o problema, ela descaracteriza um dos requisitos deste projeto. Como é desejado um número mínimo de entradas de comandos no módulo TMM (vide objetivo específico 1 na seção 4.2), a comunicação aberta entre este e a aplicação deverá ser muito bem controlada, de modo a evitar brechas para exploração de vulnerabilidades pela aplicação do medidor ou outros dispositivos. Isso é essencial, pois a "raiz de confiança" não pode ser comprometida e não

deve ter sua confiabilidade atrelada ao nível de segurança da aplicação do medidor. Além disso, um protocolo de comunicação deve ser criado e implementado pelos fabricantes de medidores, o que pode não ser um processo trivial e está sujeito a falhas.

5.8 Conclusão

Este capítulo apresentou as técnicas, elaboradas para este trabalho, com o objetivo de estipular como compor um autenticador de consumo usado em nossa arquitetura de segurança. Apresentamos também as premissas do volume de dados que devemos representar e os parâmetros de domínio apoiados em recomendações de documentos internacionais.

Em seguida, foram apresentados os resultados obtidos de maneira experimental com as técnicas de compressão de dados e, a partir deles, determinamos os melhores parâmetros utilizados em cada técnica. Com isso, concluímos que a Técnica por Contadores em Função de Dispersão é a mais apropriada para o autenticador de consumo, apresentando o menor tamanho (77 caracteres) entre os demais. Por fim, acrescentamos ao capítulo duas abordagens alternativas para a formação do autenticador de consumo.

6 Considerações Finais

Neste último capítulo da dissertação apresentamos (**i**) uma análise de segurança sobre a arquitetura proposta, (**ii**) um resumo de todo trabalho realizado e suas principais contribuições e, por fim, (**iii**) comentamos alguns trabalhos futuros.

6.1 Análise de Segurança

A arquitetura de segurança proposta neste trabalho oferece soluções para a **confiabilidade**, **autenticidade**, **integridade** e **não-repúdio** das informações de consumo calculadas pelo medidor inteligente. No entanto, questões como a confidencialidade das informações expostas pelo autenticador ACD, ataques de *replay* e garantias de disponibilidade do autenticador para o usuário não são diretamente tratadas. Além disso, o autenticador não mantém um registro temporal (*time stamping*), por não ser necessário ao problema abordado desta dissertação.

Quanto à confidencialidade das informações contidas no autenticador ACD, o esquema ECPVS especifica maneiras de construir uma mensagem recuperável confidencial, porém ao custo do **estabelecimento de um segredo** entre quem assina e o verificador. O estabelecimento e gerenciamento de um segredo para cada módulo TMM é dispendioso e torna-se dispensável para o projeto. Além disso, o papel de verificador da assinatura pode ser desempenhado por mais de uma parte interessada, o que descaracteriza a confidencialidade entre dois atores, uma vez que todos devem compartilhar o mesmo segredo.

A respeito dos ataques de disponibilidade, quando, por exemplo, o autenticador de consumo não é exibido pelo dispositivo mostrador, estes seriam prontamente detectados pelo usuário e relatados pelo mesmo à autoridade metrológica ou fiscalizadora.

De uma forma diferente, os ataques por *replay*, onde o medidor apresentaria um autenticador antigo, este não seria identificado prontamente pelo usuário, mas apenas se realizasse o Processo de Verificação da Medição. Dois pontos são importantes sobre isso, primeiramente, é o fato que o medidor malicioso não sabe, obviamente, quando um PVM está sendo realizado. Outro ponto é, caso o medidor apresentar um autenticador antigo, ele deverá também mostrar valores antigos de consumo correspondentes àquele autenticador, o que não faz sentido em um ataque a favor da distribuidora de energia.

Para qualquer tentativa da distribuidora de energia ou da aplicação do fabricante do medidor de falsificar o autenticador ACD (apresentando mais kWh nos períodos de pico, por exemplo), o atacante deverá estar ciente de que todos os ACDs seguintes ao falsificado devem estar coerentes com os ACDs verificados anteriormente, uma vez que os autenticadores carregam informações de valores de consumo acumulados. A probabilidade de falsificação é **exponencialmente inversa** ao tamanho da chave-privada e função de *hash* usados para assinar, além da redundância conhecida na mensagem embutida. A criptografia assimétrica com chaves ECC-224 oferece 112 bits de segurança (BARKER *et al.* 2012).

Em relação ao tamanho total do autenticador ACD, o *overhead* criptográfico da assinatura ECPVS poderia ser também reduzido, porém isso implicaria na **mudança do tamanho da chave** usada para assinar. Por exemplo, chaves ECC de 160 bits seriam mais adequadas para encurtar o autenticador pois gerariam um *overhead* de 20 bytes, contra 28 bytes das chaves ECC de 224 bits. No entanto, chaves baseadas em curvas elípticas de 160 bits não são recomendadas para uso após 2013 (BARKER e ROGINSKY 2011) e foram descartadas para o projeto.

6.2 Resumo do Trabalho

A Rede Elétrica Inteligente (*Smart Grid*) é um conceito amplo de uma rede integrada, sustentável e capaz de oferecer novos serviços. Desde o começo dos anos 2000, esse conceito vem ganhando força e novas redes estão sendo implementadas em todo mundo, de acordo com as necessidades de cada localidade. No Brasil, o grande motivador para a implantação das redes inteligentes é um maior controle em relação ao **furto de energia elétrica**, além do aumento na confiabilidade da infraestrutura elétrica, telemetria (medição remota) e a oferta de novos planos de tarifação para os consumidores.

Os **medidores elétricos inteligentes** são peças fundamentais para o objetivo das redes inteligentes. Para que um modelo de medidor inteligente seja comercializado em certos países, este necessita passar por um rígido processo de aprovação de modelos liderado pela **autoridade metrológica**. No entanto, esse processo vem tornando-se cada vez mais dispendioso ao passo que os medidores inteligentes adquirem mais e mais funcionalidades de *software*. No Brasil, a Portaria Inmetro nº 366 de 2011 estabelece alternativas à análise completa de código-fonte durante o processo de aprovação de modelos ao fazer menção ao uso de **arquiteturas especiais** para medidores inteligentes.

Com base nessa premissa, apresentamos uma proposta de arquitetura de segurança que oferece **confiança no comportamento** e **autenticidade dos dados** do medidor inteligente para o usuário comum e a distribuidora de energia. Além disso, essa arquitetura contribui para a **diminuição dos esforços** da autoridade metrológica durante o processo de aprovação de novos modelos de medidores e, como consequência, mitiga os riscos associados com a abertura e armazenamento de código proprietário dos fabricantes.

A proposta introduz o esboço de um mecanismo baseado em *hardware* confiável, o **Módulo de Medição Confiável** (TMM), um **Autenticador de Consumo Distribuído por Hora** (ACD) e os procedimentos externos para verificação da medição dos valores de energia consumidos, o **Processo de Verificação da Medição** (PVM). Além disso, especificamos requisitos como um baixo custo para a solução e suporte a diferentes modalidades de multitarifação de energia, o uso de Postos Tarifários.

A idéia principal está em **assinar as grandezas de consumo** no módulo de medição "o mais próximo da geração desses dados". Ou seja, o módulo TMM assina valores de kWh, calculados a partir dos dados de corrente e voltagem, no começo da cadeia de medição legalmente relevante e os envia, para o resto da cadeia, na forma de um autenticador ACD. Um novo autenticador então é disponibilizado no visor do dispositivo mostrador para cada atualização dos valores de consumo. A verificação da medição, o PVM, pode ser iniciada pelo usuário transcrevendo os valores de consumo e o autenticador ACD do visor e os inserindo como entrada em um sistema computacional para a execução do algoritmo de verificação.

Da necessidade de haver um autenticador de consumo relativamente pequeno e possível de ser manualmente transcrito, definimos o esquema ECPVS para realizar a assinatura dos dados e elaboramos quatro técnicas para a composição da mensagem embutida no autenticador ACD. Da **Técnica de Valores Absolutos**, concluímos que o autenticador ainda precisava ser diminuído e descrevemos três técnicas considerando compressão lógica de dados, sendo elas: (**i**) a **Técnica por Quantização Escalar**, (**ii**) a **Técnica por Contadores em Módulo** e (**iii**) a **Técnica por Contadores em Função de Dispersão**.

As três técnicas de compressão de dados representam os dados de consumo horário de forma diferente. A determinação do número apropriado de k bits para representação dos valores acumulados de consumo em cada registrador de hora foi realizada através de uma análise experimental. Essa análise contou com a formulação de 140 cenários para cada técnica em duas modalidades tarifárias existentes, cada cenário simulando 100 autenticadores ACD a partir de valores horários simulados de consumo. Da simulação, definimos um valor de k

apropriado para cada técnica considerando os **tempos de descompressão** e o **intervalo máximo entre o maior e menor valores de consumo** acumulado em cada hora.

Em seguida, realizamos uma análise a fim de determinar o número apropriado de bits, *h*, usado para o campo $Hash_{abs}$ da mensagem-ACD de cada técnica. O tamanho de $Hash_{abs}$ determina qual a probabilidade de se obter uma solução não-única do algoritmo de descompressão. Dessa vez, simulamos 1.000 autenticadores ACDs para cada técnica, considerando a probabilidade *p* de uma **solução não-única** deveria ser $p < 0{,}01$.

Concluímos que é possível montar um autenticador ACD através da Técnica por Contadores em Função de Dispersão com 77 caracteres, reduzindo a **70%** do tamanho da nossa primeira tentativa de compor o autenticador com a Técnica por Valores Absolutos.

Por fim, especificamos duas abordagens alternativas para um autenticador de consumo que apresentam soluções aceitáveis para o nosso problema, mas que, por outro lado, não atendem completamente aos requisitos do projeto.

6.3 Principais Contribuições

A principal contribuição desta dissertação foi a elaboração de uma arquitetura de segurança para medidores inteligentes capaz de estabelecer confiabilidade em relação às medições realizadas, em meio a um cenário de multitarifação de energia, para partes interessadas como os consumidores, as distribuidoras de energia elétrica e as autoridades metrológicas e reguladoras. A partir desta arquitetura, foi possível estabelecer uma maneira mais ágil de analisar o comportamento do *software* embarcado nos medidores inteligentes, em relação ao atual processo, o qual inclui análises de integridade e de todo código-fonte do produto.

Elaboramos um mecanismo de segurança em conformidade com os requisitos de segurança de *software* de um medidor inteligente segundo a Metrologia Legal brasileira, e que atende à última Portaria Inmetro nº 366 de 2011. Para esse mecanismo, esboçamos um módulo criptográfico e especificamos seus principais recursos e características necessárias para que ele haja como "raiz de confiança" da solução proposta. Em seguida, estabelecemos quatro técnicas para composição de um autenticador de consumo. As três técnicas considerando diferentes abordagens de compressão de dados foram simuladas e testadas para fins de análise de desempenho na verificação da mensagem embutida na assinatura e tamanho final do autenticador de consumo.

6.4 Trabalhos Futuros

Alguns aspectos relacionados aos assuntos abordados foram identificados durante o desenvolvimento do trabalho, no entanto não foram tratados com a profundidade necessária. Esses aspectos são apresentados como trabalhos futuros, estabelecendo os próximos passos para a continuidade e aprimoramento do trabalho.

Um dos possíveis aprimoramentos para a arquitetura de segurança, como um todo, é a inserção de novas funcionalidades de segurança no Módulo de Medição Confiável (TMM). Essas novas funcionalidades seriam capazes de exercer o controle de integridade do *software* embarcado, a garantia de *boot* seguro, a proteção da memória da aplicação e de parâmetros de entrada no medidor, previstos na Portaria Inmetro nº 366 de 2011. Outros mecanismos de segurança adicionais poderiam ser incluídos, como criptografia simétrica, geração de números aleatórios e *log* de eventos. Além disso, a elaboração de um protocolo para a sincronização do *Real Time Clock* poderá ser elaborada de forma mais rigorosa.

Em relação ao suporte a diferentes modalidades de tarifação horo-sazonal, um aprimoramento desejável é suportar as modalidades que configuram postos tarifários durante os fins-de-semana, porém diferentes dos postos dos dias da semana. Atualmente, o nosso mecanismo oferece suporte apenas às modalidades nas quais os fim-de-semana e feriados são contados como períodos fora-de-pico. Outra possibilidade é o suporte a cenários mais complexos, como a tarifação em tempo real, que permite variações de preços de energia em períodos curtos de tempo, como de hora em hora ou fração de hora (COUSINS 2009).

Por fim, em relação aos algoritmos de descompressão elaborados para esse trabalho, podemos destacar o uso de técnicas de programação paralela e de programação em placas gráficas para aperfeiçoar o desempenho e diminuir o tempo médio de descompressão dos dados contidos nos autenticadores de consumo.

REFERÊNCIAS BIBLIOGRÁFICAS

ABB. **Towards a smarter grid – ABB's vision for the power system of the future**. Raleigh, NC: ABB, 2009. (White Paper).

_____. **A transition from traditional to smart grids**. Mannheim, Germany: ABB's Commitment to Smart Grids, 2009. (White Paper).

AGENCIA NACIONAL DE ENERGIA ELÉTRICA (BRASIL). **Estrutura tarifária para o serviço de distribuição de energia elétrica**. Brasília: ANEEL, 2010. (Nota Técnica, 362/2010-SRE-SRD/ANEEL).

_____. **Tarifas de fornecimento de energia elétrica**. Brasília: ANEEL, 2005. (Cadernos Temáticos ANEEL, 4).

ARGOZINO, A. Tarifa branca. **Folha Press**, 2011. Disponível em: http://f.i.uol.com.br/folha/mercado/images/113321237.jpeg. Acessado em: abr. 2012.

ARORA, M. **Prevent tampering in energy meters**. 2011. Disponível em: http://www.eetimes.com/design/smart-energy-design/4014235/Prevent-tampering-in-energy-meters/. Acesso em: nov. 2011.

BARKER, E. ; ROGINSKY, A. **Transitions: recommendation for transitioning the use of cryptographic algorithms and key lengths**. Computer Security. Gaithersburg, MD: National Institute of Standards and Technology, 2011. (NIST Special Publication 800-131A).

BARKER, E. et al.; (2012). **Recommendation for key management** – Part 1: General (revision 3). Maryland: National Institute of Standards and Technology, 2012. (NIST Special Publication 800-57).

BOCCARDO, D. et al. Software evaluation of smart meters within a legal metrology perspective: a brazilian case. In: ISGT Europe - INNOVATIVE SMART GRID TECHNOLOGIES CONFERENCE EUROPE, 2010, Gothenburg, Sweden. **Proceedings ...** Piscataway, NJ: IEEE PES, 2010.

BOCCUZZI, C. V. Tecnologias de smart grid no brasil: avanços regulatórios e institucionais. In: . FÓRUM LATINO-AMERICANO DE SMART GRID, 5., 2012, São Paulo. **Anais …** São Paulo: ABDI, 2012

BONEH, D. ; LYNN, B. ; SHACHAM, H. Short signatures from the weil pairing. **Journal of Cryptology**, [S.l.], v. 17, n. 4, p. 297- 319, 2004.

BROWN, B. et al. **AMI System Security Requirements**. Raleigh, NC: UCA International Users Group, 2008. (UCAIUG: AMI-SEC-ASP)

BSI. **Anforderungen an die interoperabilität der kommunikationseinheit eines intelligenten messsystems für stoff- und energiemengen**. ed. 0.20. Bonn, Germany: Bundesamt für Sicherheit in der Informationstechnik, 2011. (Technische Richtlinie BSI TR–03109).

CAMPAGNA, M. ; ZAVERUCHA, G. **Suite E**: A cryptographic suite for embedded systems. [S.l.]: Internet Draft. Network Working Group, Certicom Corp., 2012.

CARMO, L. F. R. C. ; MADRUGA, E. L. ; MACHADO, R. C. S. Aspectos de segurança da informação em redes de medidores de energia elétrica. In: VIII Semetro - SEMINÁRIO INTERNACIONAL DE METROLOGIA ELÉTRICA, 8., 2009. João Pessoa. **Anais …** João Pessoa: UFCG/IMMETRO/SBM, 2009.

CERTICOM. Code and cipher. **Certicom's Bulletin of Security and Cryptography**, Mississauga, ON, v. 1, n. 1, p. 1-5, 2004.

_____. **Standards for efficient cryptography** 1: Elliptic curve cryptography. ed. 1.0. Mississauga, ON: Certicom Research, 2000.

_____. **Standards for efficient cryptography** 3: Elliptic curve signature schemes with partial message recovery: ECPVS and ECAOS. edição working draft 0.5. Mississauga, ON: Certicom Research, 2011.

CGEE. **Redes elétricas inteligentes**: contexto nacional. Brasília: Centro de Gestão e Estudos Estratégicos, 2011.

CHU, K.-C. **Composite dictionary compression system**. Patent US 5530645. 30 jun. 1993, 25 jun. 1996.

CLEVELAND, F. (2007). IEC TC57 Security standards for the power systems information infrastructure beyond simple encryption. In: 2005/2006 IEEE PES TRANSMISSION AND DISTRIBUITION CONFERENCE AN D EXHIBITION, 2006, Dallas, TX. **Proceedings …** Piscataway, NJ: IEEE, 2006. p. 1079-1087.

COUSINS, J. T. **Using time of use (TOU) tariffs in industrial, commercial and residential applications effectively**. Bryanston, South Africa: TLC Engineering Solutions, 2009. (White Paper).

DOE (2008). **Advanced metering infrastructure**. Washington: Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, 2008. (White Paper).

_____. **Smart grid**: an introduction. Washington, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, 2009. (White Paper).

EFTHYMIOU, C. ; KALOGRIDIS, G. Smart grid privacy via anonymization of smart metering data. In: SmartGridComm 2010 - IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS, 1., 2010. Gaithersburg , MD. **Proceedings …** Piscataway, NJ: IEEE, 2010. p. 238–243.

FEISST, C. S. D. ; FRYE, W. **Smart grid, the role of electricity infrastructure in reducing greenhouse gas emissions**. San José, CA: Cisco Internet Business Solution Group, 2008. (White Paper).

FELLER, T. ET AL. Tinytpm: a lightweight module aimed to IP protection and trusted embedded platforms. In: HOST'11 - IEEE INTERNATIONAL SYMPOSIUM ON HARDWARE-ORIENTED SECURITY AND TRUST, 2011, San Diego, CA. **Proceedings …** Piscataway, NJ: IEEE, 2011. p. 6–11.

FRANCISQUINI, A. A. **Estimação de curvas de carga em pontos de consumo e em transformadores de distribuição**. 2006. Dissertação (Mestrado em Engenharia Elétrica) - Faculdade de Engenharia de Ilha Solteira, Universidade Estadual Paulista Júlio de Mesquita Filho, Ilha Solteira, 2006.

FREITAS, F. H. ; BARRETO, P. S. L. M. ; CARVALHO, T. C. M. B. Assinatura digital para o selo verde. In: SBSEG'09 - SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 9., 2009, Campinas. **Anais …** Campinas : SBC, 2009.

GUIMARÃES, L. C. **Audiência pública 012/2006**. Associação Brasileira de Distribuidores de Energia Elétrica. Disponível em: http://www.aneel.gov.br/aplicacoes/audiencia/arquivo/2006/012/contribuicao/abradee_luiz_carlos_guimaraes.pdf. Acesso em: maio 2012.

HASHMI, M. **Survey of smart grids concepts worldwide**. [S.l.], VTT Technical Research Centre of Finland, 2011. (Technical Report)

INFINEON. **Electric metering – product brief**. 2012. Disponível em: http://www.infineon.com/smartmeter/. Acesso em: jan. 2012.

INMETRO. **Portaria Inmetro nº 011 de 13 de Janeiro de 2009**. Xerém, RJ: Instituto Nacional de Metrologia, Qualidade e Tecnologia, 2009.

_____. **Portaria Inmetro nº 366 de 16 de setembro de 2011**. Consulta Pública. Xerém, RJ: Instituto Nacional de Metrologia, Qualidade e Tecnologia, 2011.

INTEMANN, M. The common criteria approach applied to a protection profile for a smart-meter gateway. In: WORKSHOP – PROTECTION OF MEASURMENT DATA IN LEGAL METROLOGY AND RELATED CHALLENGES. 2011, Berlin. **Proceedings …** Berlin: Federal Office for Information Security (BSI), 2011.

INTERNATIONAL vocabulary of metrology – Basic and general concepts and associated terms. 3. ed. [S.l.]: Joint Committee on Guides for Metrology - JCGM, 2008. Final Draft 2006-08-01. JCGM/WG2 Document N318.

ISO/IEC. **ISO/IEC 9796-3:2006: Information technology – security techniques – digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms**. 2. ed. Genebra: International Organization for Standardization, 2006.

KATZ, J. ; LINDELL, Y. **Introduction to modern cryptography**. Boca Raton, FL: Chapman and Hall/CRC Press, 2007

LAUTER, K. The advantages of elliptic curve cryptography for wireless security. **IEEE Wireless Communications**, New York, v. 11, n.4, p. 62–67, Feb. 2004.

MCLAUGHLIN, S.; PODKUIKO, D. E MCDANIEL, P. Energy theft in the advanced metering infrastructure. In: ROME, E. : BLOOM, R. E. (Eds). **Critical Information Infrastructures Security**, 4th International Workshop CRITIS 2009, Bonn, Germany. Berlin: Springer-Verlag, 2010. p. 176–187. (Lecture Notes in Computer Science, 6027).

MENEZES, A. J.; VANSTONE, S. A. ; OORSCHOT, P. C. V. **Handbook of applied cryptography**. 1. ed. Boca Raton, FL: CRC Press, 1996.

MOLINA-MARKHAM, A. et al. Private memoirs of a smart meter. In: BuildSys'10 - ACM WORKSHOP ON EMBEDDED SENSING SYSTEMS FOR ENERGY-EFFICIENCY IN BUILDING, 2., 2010, Zürich. **Proceedings …** New York: ACM, 2010. p. 61-66.

MURRAY, J. ; VANRYPER, W. **Encyclopedia of graphics file formats**. Sebastopol, CA: O'Reilly & Associates, .1996. (O'Reilly Series).

NACCACHE, D. ; STERN, J. Signing on a postcard. In: FRANKEL, Yair (Ed) **Financial Cryptography**. 4 th International Conference on Financial Cryptography, Anguilla, British West Indies, 2000. Berlin: Springer-Verlag, 2000. p. 121–135. (Lecture Notes in Computer Science, 1962.

NCIRCLE. **Smart grid cyber security survey**. 2012. Disponível em: http://www.ncircle.com/index.php?s=resources_surveys_Survey-SmartGrid-2012. Acesso em: mar. 2012.

NIST. **Federal information processing standards publication 186-3 – digital signature standard (DSS)**. Maryland: National Institute of Standards and technology, 2009.

_____. **Framework and roadmap for smart grid interoperability standards**. Special Publication 1108. ed. 1.0. Maryland: National Institute of Standards and Technology, 2010.

NORTHEAST Group. **Brazil smart grid**: market forecast (2012 – 2022). Washington: Northeast Group LLC, 2012.

NSA. **NSA suite B cryptography**. 2011. Disponível em: http://www.nsa.gov/ia/programs/suiteb_cryptography/. Acesso em: nov. 2011.

OEB. **Electricity prices**. Ontario Energy Board. 2012. Disponível em: http://www.ontarioenergyboard.ca/OEB/Consumers/Electricity/Electricity+Prices. Acesso em: mar. 2012.

OIML D31. **Requirements of software controlled measuring instruments**. Ed. 2008 (E). Paris: International Organization of Legal Metrology. 2009.

PIKE RESEARCH. **Smart grid technologies**. Bouler, CO: Pike Research, 2009. (Technical Report).

QUINN, E. L. Privacy and the new energy infrastructure. **Social Science Research Network**, Rochester, NY, 2009. (Working Paper Series).

RADHAMANI, G. ; RAO, G. **Web services security and e-business**. Hershey, PA: Idea Group Pub., 2007

RULAND, C. E LOHMANN, T. Digital signatures based on elliptic curves in rfids. **International Journal of Computer Science and Network Security**, Seoul, v. 7, n. 1, p. 275-281, 2007.

SGIP-CSWG. **Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements**. Maryland: National Institute of Standards and Technology. 2010.

_____. **Introduction to NISTIR 7628 guidelines for smart grid cyber security**. Maryland: National Institute of Standards and Technology. 2010

STALLINGS, W. **Cryptography and network security**: principles and practice. Boston: Pearson/Prentice Hall, 2006.

TANENBAUM, A. (2002). **Computer networks**. 4. ed. Upper Saddle River, NJ: Prentice Hall Professional PTR, 2002.

TREYTL, A. ; ROBERTS, N. ; HANCKE, G. Security architecture for power-line metering system. In: WFCS 2004. IEEE INTERNATIONAL WORKSHOP ON FACTORY COMMUNICATION SYSTEMS, 5., 2004, Vienna. **Proceedings …** Piscataway, NJ: IEEE, 2004. p. 393–396.

UNITED STATES OF AMERICA. The White House. **American recovery and reinvestment act**. Washington, DC: United States Congress, 2009.

VARODAYAN, D. ; GAO, G. Redundant metering for integrity with information-theoretic confidentiality. In: SmartGridComm 2010 - IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS, 1., 2010. Gaithersburg , MD. **Proceedings …** Piscataway, NJ: IEEE, 2010. p. 345 –349.

WELMEC 7.2 Software Guide – Measuring Instruments Directive 200/22/EC. [S.l.], European Cooperation in Legal Metrology, 2008.

YAVUZ, A.; ALAGOZ, F. ; ANARIM, E. A new satellite multicast security protocol based on elliptic curve signatures. In: ICTTA'06 - INFORMATION AND COMMUNICATION TECHNOLOGIES, 2., 2006. Damascus, Syria. **Proceedings …** Piscataway, NJ: IEEE, 2006. v. 2, p. 2512–2517.